2/2019

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

42. Jahrgang
ISSN 0137-7767
12,00 Euro



■ Die Bürokratielüge ■ Ein Jahr DSGVO – Aus dem Nähkästchen ■ Kuriositäten in der [Datenschutz-]Gesetzgebung – Folge 2 ■ Quo vadis, Datenschutzbeauftragter? ■ Ein Jahr DSGVO – ein Überblick über viele Rückblicke ■ Presserklärungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Thomas Spaeing
Die Bürokratielüge – wie die Reduzierung der Benennungspflicht die Bürokratie erhöht 60

Susanne Holzgraefe
Ein Jahr DSGVO – Aus dem Nähkästchen 63

Riko Pieper
Kuriositäten in der [Datenschutz-] Gesetzgebung – Folge 2 67

Andrea Backer-Heuvedop
Quo vadis, Datenschutzbeauftragter? 75

Frank Spaeing
Ein Jahr DSGVO – ein Überblick über viele Rückblicke 78

DVD-Presserklärung vom 12.04.2019
Niedersachsen: Datenschutzfreie Regierung? 79

Offener Brief des Vereins European Digital Rights vom 15.05.2019 an die Europäische Kommission 80

DVD-Presserklärung vom 04.06.2019
#StopSpyingOnUs: Kampagnenstart in 9 EU-Ländern gegen rechtswidrige Online-Werbemethoden 83

Datenschutznachrichten

Deutschland 84

Ausland 95

Technik-Nachrichten 107

Rechtsprechung 108

Buchbesprechungen 113

Termine



Foto: Pixabay..com

Donnerstag, 01. August 2019
Redaktionsschluss DANA 3/2019
Real Time Bidding

Sonntag, 08. September 2019
Vorstandssitzung der DVD in Kiel
Interessierte melden sich bitte in der Geschäftsstelle der DVD an.

Montag, 09. September 2019
Sommerakademie des ULD Schleswig-Holstein
https://datenschutzzentrum.de/sommerakademie/2019/

Samstag, 26. Oktober 2019
DVD-Vorstandssitzung
Bonn

Sonntag, 27. Oktober 2019
DVD-Mitgliederversammlung
Bonn

Freitag, 01. November 2019
Redaktionsschluss DANA 4/2019
Datenschutz in Zeiten des Brexit – Auslands-Datenverarbeitung (Arbeitstitel)

DANA
Datenschutz Nachrichten
ISSN 0137-7767
42. Jahrgang, Heft 2

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Frank Spaeing
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autorinnen und Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, Pixabay, Wikipedia

Editorial



Ein Jahr DSGVO – Entwicklungen, Erfahrungen, Baustellen

Nach einem Jahr DSGVO wollten wir uns eigentlich nur über die Erfahrungen mit der DSGVO unterhalten und vielleicht noch die damit einhergehenden Kuriositäten beleuchten.

Aber leider wird – unabhängig davon, wie oft der deutsche Gesetzgeber in der Vergangenheit auf dem Weg zur DSGVO schon das Datenschutzrecht geschwächt hat – schon wieder versucht den Datenschutz in Deutschland drastisch zu beschneiden.

Dieses Mal unter dem Mäntelchen des Bürokratieabbaus, bei dem passend gleich die Rolle der Datenschutzbeauftragten mit abgebaut werden soll.

Deswegen wird in diesem Heft die Bürokratielüge entlarvt, berichtet eine Datenschutzberaterin aus dem Nähkästchen, bekommen Sie den zweiten Teil der Serie über Kuriositäten in der (Datenschutz-)Gesetzgebung vorgelegt, wird die Entwicklung und die Bedeutung der Datenschutzbeauftragten in Deutschland und Europa dargestellt und geben wir Ihnen einen kurzen Überblick über mehrere Fazits und Resümees und Gutachten zu einem Jahr DSGVO.

Außerdem stellen wir unsere Beteiligung an Kampagnen und offenen Briefen dar und drucken unsere Pressemitteilungen des letzten Quartals ab.

Die Nachrichten aus dem In- und Ausland sowie zu Technikthemen, Aktuelles aus der Rechtsprechung und Buchbesprechungen runden das Heft in gewohnter Weise ab.

Wir wünschen Ihnen eine spannende Lektüre in diesen frühsommerlichen Tagen!

Frank Spaeing

Autorinnen und Autoren dieser Ausgabe:

Andrea Backer-Heuveldop
Dipl.-Betriebswirtin / LL.M., Externe Datenschutzbeauftragte, andrea.heuveldop@ds-quadrat.de, Dissen

Markus Eßfeld
Vorstandsmitglied in der DVD, essfe ld@datenschutzverein.de

Susanne Holzgraefe
Vorstandsmitglied in der DVD, holzgraefe@datenschutzverein.de

Riko Pieper
Vorstandsmitglied in der DVD, pieper@datenschutzverein.de

Frank Spaeing
Vorstandsmitglied in der DVD, spaeing@datenschutzverein.de

Thomas Spaeing
Vorstandsvorsitzender des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V., thomas.spaeing@bvdnet.de

Thomas Spaeing

Die Bürokratielüge – wie die Reduzierung der Benennungspflicht die Bürokratie erhöht

Bürokratieabbau ist das große Ziel und Datenschutz soll das kleine Opfer sein. Die Bürokratisierungsexperten aus CDU/CSU und der FDP wollen die Bürokratie bei den kleinen und mittleren Unternehmen abbauen. Dazu sollen aber nicht etwa beispielsweise das überbordende Baurecht oder das im weltweiten Vergleich ausufernde Steuerrecht verschlankt werden, sondern beim Datenschutz soll abgebaut werden.

Die unglückliche und kaum medial vorbereitete Einführung der DSGVO hat zu einem erheblichen Chaos insbesondere in der mittelständischen Wirtschaft und im Vereinswesen geführt. Die negative Presseberichterstattung hat dazu ebenfalls beigetragen. Viele Unternehmer oder Vereinsvorstände fühlten sich erheblich verunsichert und zu Unrecht bedroht – von Bußgeldern und Abmahnungen gleichermaßen. Dass dies vollkommen übertrieben war, hat sich inzwischen gezeigt. Das durchschnittliche Bußgeld in Deutschland liegt bisher sogar unter den Werten der Zeit des alten Datenschutzrechts und Abmahnungen sind ebenfalls kaum bekannt.

Für Wahlversprechen werden Bürgerrechte geschwächt

Trotzdem sind Teile der Bundesregierung in das Wehklagen eingestiegen und haben offenbar Zusagen gemacht, die leider nicht so einfach einzuhalten sind. Die DSGVO ist EU-Recht und das kann natürlich Deutschland allein nicht ändern. Aus diesem Grund hat man sich den Teil ausgesucht, den man in Deutschland ändern kann: Die Öffnungsklauseln zum Datenschutzbeauftragten.

Der Datenschutzbeauftragte wurde 1977 als Instrument der betrieblichen und behördlichen Selbstkontrolle eingeführt, um neben den Datenschutzaufsichtsbehörden die Einhaltung des Datenschutzrechts zu gewährleisten. Das hat, soweit die Unternehmen dies so umgesetzt haben, gut funktioniert. Deutsche Unternehmen sind hier längst weltweit führend.

Nach Erkenntnissen des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.[1] wurde das alte Datenschutzrecht von etwa 40 % der Unternehmen umgesetzt und auch gewissenhaft in die DSGVO überführt[2]. Eine Reihe weiterer Unternehmen hat dies mehr schlecht als recht getan und ein ebenfalls beachtlicher Teil von über 30 % der Unternehmen hat nichts getan. Diese Unternehmen haben bis heute nichts getan und dabei sicherlich einiges gespart. Gleichfalls haben diese Unternehmen aber auch gegen geltendes Recht verstoßen. Da aber das Risiko und die Bußgelder überschaubar waren, hat dies nur wenig Aufsehen verursacht. Nun, da die Bußgelder höher ausfallen könnten und Ungemach auch von anderer Seite drohen könnte (Schadensersatzforderungen, Abmahnungen, ...), möchten diese Unternehmen durch die Politik geschützt werden – und die ist in Gestalt einiger CDU/CSU- und FDP- Politiker auch sofort zur Stelle. Nicht um die Bürger zu schützen oder dem Recht Geltung zu verschaffen, sondern um denjenigen Unternehmen, die sich an das bereits seit 1977 geltende Datenschutzrecht nicht gehalten haben, auch für die Zukunft einen Freibrief auszustellen. Vergleichbares ist im Bau- oder Steuerrecht undenkbar.

Wie mag sich da der Unternehmer fühlen, der sich selbstverständlich an dieses Recht gehalten hat? Auch bei den Bürgern findet diese Vorgehensweise sicher wenig Verständnis und ist genau die Art von Politik, die zu einer zunehmenden Entfremdung führt.

Was ich nicht weiß, macht mich nicht heiß

Unwissenheit schützt vor Strafe nicht. Dies einmal vorausgesetzt, kann das heimliche Hauptargument zahlreicher Akteure gleich entkräftet werden: Der Datenschutzbeauftragte zeigt auf, was alles im Unternehmen beim Datenschutz schief läuft, das macht den Unternehmer bzw. die Leitung des Verantwortlichen dann im juristischen Sinne „bösgläubig" – er wusste um den Verstoß und hat ihn doch nicht abgestellt. Natürlich macht sich das im Bußgeldverfahren oder auch bei einer Straftat nicht gut.

Wenn man nun diesen „Überbringer der schlechten Nachricht" (den Datenschutzbeauftragten) entfernt, dann wäre doch alles viel besser. Tja, wäre da nicht der Satz aus der Überschrift. Unwissenheit schützt vor Strafe nicht. Auch ohne einen Datenschutzbeauftragten und ggf. ohne zu wissen, dass man gegen ein Gesetz verstoßen hat, kann man dafür bestraft werden. Die DSGVO legt eindeutig fest, wer für das Thema verantwortlich ist: Der Verantwortliche, bzw. dessen Leitung. Dieses „Ich will es gar nicht wissen..."-Argument ist also falsch und zeigt die eigenartige Denkweise mancher Akteure.

Bürokratie wird mehr, wenn es keinen Sachverstand gibt

Nun aber zum Kernpunkt: Wird Bürokratie abgebaut, wenn Datenschutzbeauftragte nicht benannt werden müssen? Nein, welche auch? Die DSGVO, das BDSG sowie sämtliche anderen Datenschutzvorschriften sind vollumfänglich zu erfüllen. Dies gilt – auch ohne Datenschutzbeauftragte – weiterhin für alle Unternehmen und Vereine, seien diese auch noch so klein. Allerdings würden mit den Datenschutzbeauftragten diejenigen entfernt, die helfen könnten, dieses Recht risikobasiert und angemessen umzusetzen. Statt dessen werkeln dann fachfremde Personen an Einwilligungserklärungen und Verträgen, schreiben Dokumentationen und schulen mehr schlecht als Recht Mitarbeiter.

Dies alles ist bereits passiert und ohne die Datenschutzbeauftragten werden wir davon noch viel mehr erleben: Falsche und unnötige Einwilligungserklärungen, unsinnige Unterschriften zu allen möglichen Zwecken, untaugliche Verträge und überbordende Dokumentationen gab es seit dem 25.05.2018 schon zuhauf, weil es nicht genug qualifizierte Datenschutzbeauftragte gab, um den Beratungsbedarf zu decken.

Eines der bewährtesten Mittel, um Bürokratie im Datenschutz zu vermeiden, sind qualifizierte Datenschutzbeauftragte. Die Schwächung der Benennungspflicht ändert an der Bürokratie in den Unternehmen nur insoweit etwas, als dass diese zunehmen wird. Auf jeden Fall steigen die Risiken für die Verantwortlichen gegen die Regelungen zum Datenschutzrecht zu verstoßen.

Ganz nebenbei: Wenn keine Datenschutzbeauftragten benannt werden, sind die Geschäftsführungen selbst für deren Aufgaben verantwortlich. Dergleichen wird auch immer wieder ins Feld geführt: „Das mache ich als Geschäftsführer selbst." – Wenn dafür Zeit ist und die Expertise vorliegt, kann das ein gangbarer Weg sein. Die Praxis zeigt aber, dass dies ein Irrtum ist, ein Geschäftsführer oder Vorstand hat für diese Themen weder Zeit noch die notwendigen Kenntnisse. Und ganz unabhängig davon gilt es ja noch das Problem des Interessenkonflikts[3] zu umgehen.

Wie sehen das Kunden und Mitarbeiter?

Gleichzeitig steht es um die Betroffenenrechte in diesen Unternehmen schlecht. Mit welcher Begründung werden die Rechte von Beschäftigten in diesen Unternehmen bewusst geschwächt? Sind sie Mitarbeiter zweiter Klasse? Und die Kunden, wie steht es um diese? Sollen die besser gleich zum größeren Wettbewerb gehen, weil für den die strengeren Regelungen gelten und man dort sicher sein kann, dass die Daten besser geschützt werden?

Wir merken schon, das bekommt einen ganz seltsamen Drive. Natürlich wollen wir gerade das nicht. Auch in kleinen Unternehmen sollen die Mitarbeiter nicht unkontrollierten Überwachungsmaßnahmen ausgesetzt sein und auch Kundendaten sollen dort gut geschützt werden. Wir erinnern uns: WhatsApp hatte zum Zeitpunkt des Verkaufs an Facebook gerade mal 50 Mitarbeiter aber etwa 800 Millionen Kunden. Sollte Datenschutz hier eine Rolle spielen? Keine Frage!

Es wird zwar immer wieder behauptet, dass Kunden für coole kostenlose Services und Apps gerne mit ihren Daten bezahlen, aber das stimmt nur dann, wenn der Datenschutz passt. Kunden geben immer wieder an, dass sie voraussetzen, dass Anbieter sich an die Regeln halten – und genau dass will ja auch die DSGVO. Datenschutzbeauftragte tragen zur Vertrauensbildung bei – dies kommt dem Image des Unternehmens und seinen Produkten und Dienstleistungen entgegen. Hinzu kommt, dass Kunden die Datenverarbeitungsmechanismen hinter den kostenlosen Services meist gar nicht verstehen. Wenn man sie dann aufklärt, ändern viele Nutzer ihr Verhalten und wechseln bspw. zu datenschutzfreundlicheren Varianten wie Threema statt weiter WhatsApp zu nutzen.

Selbst Schüler, die der BvD im Rahmen seiner Initiative „Datenschutz geht zur Schule" im Bereich Medienkompetenz sensibilisiert, ändern nach Erhebungen an den Schulen normalerweise ihr Verhalten bei der Mediennutzung nachhaltig. Es mangelt also nicht am Wollen, sondern am Können bzw. Wissen. Medienkompetenz wird in Deutschland an den Schulen, im Studium und auch in der Berufsausbildung wenig bis gar nicht vermittelt. Ein wichtiges Tätigkeitsfeld für die Bildungspolitiker der Bundesländer und auch die Bundesregierung. Hier spielt Deutschland leider in der dritten Liga!

Chancen durch Datenschutz nutzen!

Von dieser Seite betrachtet, wird schnell deutlich, dass die Schwächung der Benennung eines Datenschutzbeauftragten auch eine Schwächung der Unternehmen ist. Die Unternehmensprozesse zu durchleuchten, um zu ermitteln wie und warum personenbezogene Daten von Kunden und Beschäftigten verarbeitet werden, führt regelmäßig zu einer Reihe wichtiger Erkenntnisse, die helfen die Datenverarbeitung schlanker, sicherer und oft transparenter zu machen. Regelmäßig werden Prozesse deutlich sicherer, denn in fast jedem Unternehmen haben sich unnötige Prozesse, Verarbeitungen oder Berechtigungen eingeschlichen. Die deckt ein erfahrener Datenschutzbeauftragter auf und hilft somit Komplexität zu reduzieren, Kosten zu senken und besser zu werden. Klassische Ziele eines Re-Engineering-Prozesses – ganz nebenbei.

Noch besser: Die Erkenntnisse und die Sicherheitsmaßnahmen aus diesem Prozess kommen allen anderen Datenverarbeitungen auch zugute. Verschlüsselungsmaßnahmen schützen auch Geschäftsgeheimnisse und geschulte Mitarbeiter gehen Hackern und Angreifern nicht so schnell auf den Leim. Hier haben Unternehmen und Behörden in Deutschland bereits genug schlechte Erfahrungen gesammelt – und die Politik auch[4]. Es werden also ganz konkret Maßnahmen ergriffen, die die Wettbewerbsfähigkeit eines Unternehmens stärken und seine Produkte sicherer machen können.

Wollen wir in diesem Marktumfeld kleine oder neue Unternehmen stärken, so helfen wir ihnen von Anfang an compliant zu arbeiten und sichere Lösungen und Dienstleister einzusetzen. Weitsichtig wären hier entsprechende Informations- und Förderprogramme für Start-Ups und KMU. Das stärkt die Wirtschaft nachhaltig und hilft den Unternehmen die Anforderungen größerer (ggf. auch internationaler) Kunden zu bestehen. Denn die Kunden und Aufsichtsbehörden anderer Länder haben wenig Verständnis dafür, dass hier in Deutschland mit zweierlei Maß gemessen werden soll. Wenn erst ein Auftrag verloren ging, weil es am Datenschutz gefehlt hat, dann ist es zu spät.

Nicht ohne Grund arbeitet beispielsweise die Automobilindustrie bereits an eigenen Datenschutz-Vorgaben und -Zertifizierungen von Lieferanten, um deren Zulieferung abzusichern. Ein Zulieferer, der mit Datenschutz- oder Datensicherheitsproblemen kämpft, ist für seine Kunden ein Risiko. Nicht nur, dass bspw. Daten verloren gehen können, die Lieferprozesse und damit die eng getaktete Produktionskette werden beeinträchtig oder kommen gar zum Stillstand.

Hier setzen künftig genau dieselben Mechanismen ein, wie sie aus dem Qualitätsmanagement bekannt sind. Auch in anderen Branchen sind Datenschutzaudits bei Zulieferern und Dienstleistern längst Standard. Wer nicht mithalten kann, bekommt den Auftrag nicht. Erschreckend oft sind dies junge Start-Ups, die ihre tollen Ideen im rechtsfreien Raum gedacht und entwickelt haben. Wenn dann die Compliance-Anforderungen der Kunden kommen, reagieren sie mit Unverständnis. Das ist ein Versagen der Wirtschaftspolitik. Wir müssen diese Unternehmen besser auf die Anforderungen vorbereiten anstatt sie in einen luftleeren rechtsfreien Raum zu stellen. Wir befreien Start-Ups auch nicht von den Anforderungen des Bau- oder Steuerrechts – um im Bild zu bleiben.

Datenschutz managen

Das bringt uns zu einem Aspekt, der mit der DSGVO so neu auf den Plan getreten ist: Datenschutz managen. Von einem Datenschutzmanagement wurde auch früher schon viel gesprochen. Aber erst die DSGVO mit den Regelungen zur Rechenschaftspflicht aber auch zur Zertifizierung bereitet den Boden für ein Datenschutzmanagementsystem. Hier liegt auch für die Unternehmen ein gewaltiges Potential. Genau wie beim Qualitätsmanagement skaliert ein Unternehmen sein Datenschutzmanagement und dessen Komplexität passend zu seinen Prozessen und Datenverarbeitungen. Hier ermöglicht die am Risiko orientierte DSGVO den Unternehmen genau die Komplexität abzubilden, die erforderlich ist, und eben nicht mehr.

Sicher, die eine oder andere Dokumentations- und Transparenzpflicht mutet im Mittelstand unnötig und bürokratisch an. Aber genau hier hilft wiederum der qualifizierte Datenschutzbeauftragte, um den Aufwand im Rahmen zu halten und nur die tatsächlich notwendigen Pflichten angemessen zu erfüllen.

Ein solcher Datenschutzbeauftragter unterstützt das Unternehmen auch dabei, ein Datenschutzmanagement aufzubauen. Das klingt nach viel Aufwand, ist aber vor allem für QM-erfahrene Unternehmen meist schnell erledigt. Zunächst werden die erforderlichen Datenschutz- und Verarbeitungsprozesse beschrieben, dann wird festgelegt, wer innerhalb der Prozesse für welche Tätigkeiten zuständig ist und daraus ergeben sich letztlich die notwendigen Arbeitsanweisungen, die den Mitarbeitern vermittelt und zugänglich gemacht werden müssen. Nach den Schulungen werden regelmäßige Audits durch den Datenschutzbeauftragten oder entsprechend geschulte Mitarbeiter durchgeführt. Die Ergebnisse aus den Audits werden der Leitung (Geschäftsführung/Vorstand) berichtet und diese legt die notwendigen Abstellmaßnahmen fest und durch wen diese zu erfolgen haben.

Das war's schon fast, der PDCA-Zyklus (Plan, Do, Check, Act), wie er im Qualitätsbereich hinreichend bekannt ist, übertragen auf den Datenschutz. Die so geschaffene Organisation beherrscht das Thema und ist jederzeit in der Lage einer Aufsichtsbehörde oder einem Kunden nachzuweisen, dass der Datenschutz funktioniert.

Noch viel einfacher – weil wieder am Risiko orientiert – lässt sich der Datenschutz in Handwerksbetrieben und im kleinen Handel realisieren. Hier sind eben Erfahrung und Augenmaß gefordert und nicht rechtstheoretische Abhandlungen, wie sie in mancher Rechtsberatung immer wieder entstehen.

Wie findet man einen qualifizierten Datenschutzbeauftragten?

Natürlich müssen wir an dieser Stelle noch über den Datenschutzbeauftragten sprechen. Wenn hier von einem qualifizierten Datenschutzbeauftragten die Rede ist, dann ist das nicht der selbsternannte Experte, der stets nur die halbe Buchseite weiter ist als sein Kunde. Ein Tageslehrgang macht noch keinen Datenschutzbeauftragten und ein Wochenlehrgang noch keinen Berater.

Ein qualifizierter Datenschutzbeauftragter ist solide vorgebildet in den Bereichen Informationstechnik, Betriebswirtschaft und Unternehmensorganisation und im Bereich Datenschutzrecht. Datenschutzbeauftragte sind oft Quereinsteiger aus einem dieser Bereiche und haben sich die anderen Fähigkeiten angeeignet. Interne Datenschutzbeauftragte können durchaus weniger umfassend qualifiziert starten, wenn sie dafür das Unternehmen gut kennen, denn auch dieses Wissen ist für die Tätigkeit sehr relevant.

Hingegen müssen externe Datenschutzbeauftragte, da sie ja das Unternehmen nicht kennen, mehr Erfahrungen und von Anfang an eine hohe Qualifikation in allen genannten Bereichen haben und insbesondere die erforderliche Beratungskompetenz mitbringen.

Das Problem der Unternehmen ist es die passende Lösung für sich zu ermitteln und dabei nicht den zahlreichen Blendern auf den Leim zu gehen, die der DSGVO-Boom leider auch hervorgebracht hat. Der BvD entwickelt dazu momentan ein Beratungsangebot für Unternehmen und Behörden, das helfen soll die jeweils richtige Lösung zu finden.

Um bei der Beratung die Spreu von dem Weizen zu trennen, müssen Ausbildung und Berufsausübung standardisiert werden. Mit dem Beruflichen Leitbild des Datenschutzbeauftragten[5] hat der BvD hier bereits vorgelegt. Der nächste sinnvolle Schritt ist eine Berufszertifizierung durch eine neutrale Stelle. Also nicht durch den Ausbilder, sondern wie bspw. in Frankreich durch die CNIL – also die zuständige Aufsichtsbehörde. Allerdings wird in Frankreich die Berufsausübung noch nicht in die Zertifizierung einbezogen, d.h. das Zertifikat trifft noch keine Aussage darüber, ob der geprüfte Datenschutzbeauftragte die Kenntnisse auch in die Tat umsetzt. Diesen Anspruch hat das Berufsbild und so sollte auch der Standard für eine Zertifizierung in Deutschland aussehen. Dies gibt den Unternehmen die notwendige Sicherheit bei der Auswahl des richtigen Mitarbeiters oder Beraters. Hier ergibt sich ein weiteres sinnvolles und dringendes Handlungsfeld für die Politik.

Fazit

Wenn es eigenen Zwecken dient, dann ist der Datenschutz stets eine hochwillkommene Rüstung gegen die Presse oder wissbegierige Bürger. Wenn es ein bisschen Gegenwind gibt, dann wird schnell über die unnötige Bürokratie gejammert. Diese Bürokratie gibt es natürlich wie in vielen Gesetzen so auch im Datenschutzrecht. Die Datenschutzbeauftragten gehören allerdings ganz sicher

nicht dazu. Wie Steuerberater in ihrem Bereich helfen sie mit ihrem Know-how Bürokratie zu vermeiden und die Anforderungen zum Datenschutz so effizient wie möglich umzusetzen. Wenn die Politik handeln möchte, so haben wir nun einige wichtige Bereiche gesehen, die schon lange auf Handlungsfähigkeit warten. Die Heilsversprechen zum Bürokratieabbau durch die Anpassung der Benennungspflicht wären ein „Danaergeschenk" – das niemand wirklich will.

Der BvD hat im Übrigen pragmatische Vorschläge zur schnellen Entlastung von Unternehmen und Vereinen vorgelegt (siehe www.bvdnet.de, Stichwort Positionspapiere).

1 Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. fördert und vertritt die Interessen der Datenschutzbeauftragten in Betrieben und Behörden. Der Verband unterstützt seine Mitglieder bei der täglichen Berufsausübung und entwickelt die Standards für die Berufsausübung weiter.

2 https://www.bvdnet.de/ds-gvo-wichtige-handlungsfelder-fuer-unternehmen/

3 https://www.datenschutz-wiki.de/DSGVO:Art_38, dort Absatz 6, 2. Satz, siehe außerdem: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/03/Beschluss-des-D%C3%BCsseldorfer-Kreises-2010-Mindestanforderungen_an_DSB_nach_4f_II_und_III_BDSG.pdf

4 https://www.zeit.de/politik/deutschland/2019-01/hackerangriff-politiker-leak-daten-dokumente-twitter

5 https://www.bvdnet.de/berufsbild/

Susanne Holzgraefe

Ein Jahr DSGVO – Aus dem Nähkästchen

Endlich ist er da, der 25. Mai 2018. Die DSGVO tritt in Kraft. Endlich kein Tracking unseres Verhaltens im Internet mehr, endlich müssen Auskunfteien Ergebnisse für Betroffene nachvollziehbar gestalten, endlich keine Videoüberwachung in U-, S- und Regionalbahnen mehr, endlich noch mehr Transparenz, endlich Aufklärung in leicht verständlicher und möglichst einfachen Sprachen, endlich ... Die Erwartungen vieler Bürger waren hoch. Die DSGVO brachte auch die Hoffnung, dass jetzt endlich Gesetze, die es schon vorher gab, umgesetzt würden. Immerhin hat sich zum vorherigen Bundesdatenschutzgesetz (BDSG) ja gar nicht so viel geändert.

Doch überrollte uns alle zuerst einmal eine E-Mail-Flut. Tausende und Abertausende an E-Mails bezüglich Einwilligungen in irgendwelche Newsletter wurden versandt. Betrüger sprangen auf diesen Zug auf. Viele der E-Mails entpuppten sich als sogenannte Fishing-Mails. Für die Versendung von Newslettern war auch nach altem Recht schon eine Einwilligung der Betroffenen notwendig. Für die meisten Unternehmen und Organisationen änderte sich daher nichts. Hier wurde lediglich noch einmal das Bewusstsein geschärft, dass die Versendung von Newslettern und anderer Direktwerbung einer Einwilligung bedarf. Die Angst vor Abmahnanwälten ließ hier einige handeln, die vorher die Gesetze und Vorschriften zum Datenschutz noch nicht umgesetzt hatten.

Direkt nach der Newsletter-Einwilligungs-Welle folgte die Cookie-Banner-Welle. Hier versuchten einige viel Geld zu verdienen, indem sie Software für nicht legale Cookie-Banner verkauften. Traurigerweise verbreiteten sich die illegalen Cookie-Banner im Fluge. Viele Verantwortliche vertrauten ihren Webdesignern und befassten sich augenscheinlich nicht selbst mit der Gesetzeslage, oder sie vertrauten darauf, dass es für falsche Cookie-Banner so geringe Bußgelder gibt, dass sich die illegalen Cookie-Banner zur Kundengewinnung trotz Bußgelder rechnen. Viele Webdesigner vertrauen wiederum den Anbietern der Software, die sie für die Cookie-Banner einsetzen, statt sich selbst mit der Gesetzeslage auseinanderzusetzen. Bis heute sind die illegalen Cookie-Banner weit verbreitet. Es gibt nach wie vor Webdesign-CMS-Software, die mit illegalen Cookie-Bannern ausgeliefert wird. Hier ist also Vorsicht geboten und es sollte genau geprüft werden, ob der eingesetzte Cookie-Banner den gesetzlichen Anforderungen entspricht.

Nach wie vor sind sich auch der eine oder andere Webdesigner der Folgen für den Verantwortlichen nicht bewusst, wenn sie zu falschen Cookie-Bannern raten oder sie im Auftrag einbauen. Natürlich können sich Webdesigner gegen Beratungs- und Planungsfehler versichern. Die Verantwortung und somit die Haftung liegt bei dem Verantwortlichen, also bei dem Unternehmen bzw. der Organisation, für die mit der Webpräsentation geworben wird.

Immer wieder wurde die DSGVO im letzten Jahr verteufelt. In öffentlichen Diskussionen kam immer wieder das Argument: „Besonders hart würde es die Handwerker treffen." Tatsächlich jedoch hatte die Handwerkskammer vorgesorgt. Es fiel auf, dass keine andere Kammer ihre Mitglieder so gut auf die DSGVO vorbereitet hatte, wie die Handwerkskammer. Immer wieder tauchten in der Presse Berichte über Fotografen auf, die sich beschwerten, dass sie jetzt eine Einwilligung von Betroffenen bräuchten und alles so schwierig geworden sei. Interessanterweise ist das, was die Fotografen beklagten, aber gar nicht neu gewesen.

Ein Aufschrei ging auch durch viele Vereine und Parteien. Dabei hatte sich die Gesetzgebung auch für Vereine und Parteien gar nicht so stark geändert. Es war eher der Aufschrei des Bewusstwerdens, dass auch Vereine und Parteien Gesetze und Vorschriften rund um den Datenschutz einhalten sollten. Datenschutz gehört in Vereinen und Parteien

genauso zu der Compliance, mit der sich ehrenamtliche Vorstände befassen sollten, wie es in Unternehmen die Pflicht der Geschäftsleitung ist.

Bürger suchen Rat

Seit vielen Jahren engagiere ich mich in einem Verein für Bürgerrechte zum Thema Datenschutz. Wir bekamen immer schon Anfragen von ratsuchenden Personen. Häufig waren es Beschäftigte mit ziemlich heftigen Fällen. Aber natürlich gab es auch andere Fälle. Im Grunde lassen sich die Anfragen in drei Kategorien einteilen: Entweder ist aus datenschutzrechtlicher Sicht alles in Ordnung, es ist ein Fall für die Spam-Beschwerdestelle oder es ist ein Fall für den Datenschutzbeauftragten des Verantwortlichen beziehungsweise für die zuständige Aufsichtsbehörde. Wir raten immer zuerst das vertrauliche Gespräch mit dem Datenschutzbeauftragten des Verantwortlichen zu suchen, sofern es einen gibt. Da früher die Kontaktdaten der Datenschutzbeauftragten in der Regel nicht veröffentlicht wurden und selbst Beschäftigte häufig nicht darüber informiert wurden, wie sie den Datenschutzbeauftragten des Unternehmens erreichen können, haben wir in solchen Fällen die Kontaktdaten beim Verantwortlichen nachgefragt und an die Betroffenen weitergeleitet. Seit Mai 2018 lässt sich in der Regel in der Datenschutzerklärung auf den Webpräsentationen der Firmen ein Kontaktdatum zur Erreichung des Datenschutzbeauftragten finden. Allerdings ist es meistens eine E-Mail-Adresse, die wenig Aufschluss darüber gibt, wer die an diese Adresse geschickten E-Mails alles mitlesen kann.

Vertraulichkeit von Datenschutzbeauftragten

Die Datenschutzerklärungen vieler Webpräsentationen geben über die Empfänger der angegebenen E-Mail-Adressen zu Verantwortlichen und Datenschutzbeauftragten häufig keinen Aufschluss. Wünschen Betroffene ein vertrauliches Gespräch, schreiben wir die E-Mail-Adresse des Datenschutzbeauftragten an und bitten um die Bereitstellung eines Schutzraumes für ein vertrauliches Gespräch mit Betroffenen. Hierbei machten wir spannende Erfahrungen. Immer wieder mussten wir feststellen, dass es leider eine Reihe Datenschutzbeauftragte gibt, denen §38 Abs. 2 BDSG bzw. §6 Abs. 5 Satz 2 BDSG (Verschwiegenheitspflicht) nicht bekannt war. Immer wieder mussten wir feststellen, dass die Kommunikation mit dem betrieblichen Datenschutzbeauftragten an die Verantwortlichen weitergeleitet wurde. Die Fälle, in denen dieses durch die Betroffenen den zuständigen Behörden gemeldet wurde, wurden von den Behörden sehr zügig behandelt und sie teilten den Betroffenen mit, dass sie mit den Verantwortlichen gesprochen haben. Der eine oder andere Datenschutzbeauftragte entschuldigte sich dann auch bei den Betroffenen.

Ein Datenschutzbeauftragter antwortete, nachdem die Betroffenen das Fehlverhalten angesprochen hatten, dass er doch selbstverständlich den Geschäftsführer in CC setzen müsse, denn es sei ja schließlich sein Chef.

In durchaus vielen Fällen, in denen die Betroffenen den entsprechenden Datenschutzbeauftragten auf sein Fehlverhalten angesprochen hatten, kam die Antwort: „Ich muss aber doch prüfen, ob sie überhaupt Kunde des Unternehmens sind.“ Natürlich dürfen sich nicht nur Kunden vertraulich an den Datenschutzbeauftragten wenden.

Es waren nicht nur kleinere Unternehmen, bei denen die Kommunikation mit dem Datenschutzbeauftragten an andere Personen des verantwortlichen Unternehmens gingen. Selbst ein Unternehmen aus der Erotikbranche war dabei. Der Vorfall hat uns ziemlich verwundert, denn das Unternehmen ist ansonsten für seine Diskretion bekannt. Da die Betroffenen es als nicht so schlimm empfanden, meldeten sie den Vorfall nicht der Behörde, sondern suchten das Gespräch. Der Datenschutzbeauftragte bat um ein Telefonat, um die Sache zu klären. Es stellte sich heraus, dass er auf Grund einer extrem hohen Zahl von Anfragen, die bei ihm eingehen, für die er aber der falsche Adressat ist, die Anfrage der Betroffenen im Eifer des Gefechts versehentlich weitergeleitet hatte.

Bei einem großen Elektronikmarkt wendeten sich Betroffene an die E-Mail-Adresse des Datenschutzbeauftragten, die auf den Webseiten sowie den Informationen zur Videoüberwachung am Markt angegeben waren. Nach acht Wochen bekamen sie eine Antwort vom Kundenservice, dass man hoffe, dass sie mit der gekauften Ware zufrieden seien. Das bedeutet, dass die angegebene E-Mail-Adresse tatsächlich im Ticketsystem des Kundenservice landet, wo sie von einer uns unbekannten Anzahl Beschäftigten eingesehen werden kann; Beschäftigte oder gar Auftragsverarbeitende? Callcenter? Ein Ticketsystem, in dem darüber hinaus üblicher Weise nicht nur Admins mitlesen können, sondern häufig auch der Vertrieb, Marketing und die Geschäftsleitung. Wer genau mitliest, wurde in der Datenschutzerklärung auf der Webseite, auf der wir die E-Mail-Adresse gefunden hatten, nicht angegeben, obwohl Art. 13 DSGVO vorschreibt, dass die Empfänger bzw. Kategorien der Empfänger genannt werden müssen. Die zuständige Behörde kümmerte sich postwendend, nachdem die Betroffenen sie einschalteten, konnte aber kein Fehlverhalten feststellen. Auch fast ein Jahr später warten die Betroffenen immer noch auf die Antwort des Datenschutzbeauftragten zur eigentlichen Frage.

Bei einem Lieferservice stand auf den Webseiten für den Verantwortlichen und den Datenschutzbeauftragten dieselbe E-Mail-Adresse. Als ich die angegebene Telefonnummer des Verantwortlichen anrief, um nach den Kontaktdaten zu fragen, landete ich in einem Callcenter, das augenscheinlich den Kundenservice für mehrere Lieferdienste übernahm, denn sie nannten mir die Kontaktdaten des Datenschutzbeauftragten eines anderen Unternehmens. Erst auf erneute Nachfrage bekam ich die richtigen Daten. Der Datenschutzbeauftragte, den ich daraufhin selbst kontaktierte, war ziemlich entsetzt. Das Unternehmen wurde in der Zwischenzeit aufgekauft und hat heute auf seinen Webseiten einen Datenschutzbeauftragten mit Sitz in den Niederlanden stehen.

Die Betroffenen machten auch die Erfahrung, dass es Datenschutzbeauftragte gibt, die keine Anfragen von Betroffenen entgegen nehmen. Sie teilten den Betroffenen mit, dass sie zwar Datenschutzbeauftragte des Verantwortlichen seien, aber Gespräche zum Thema

Datenschutz würde der Verantwortliche selbst führen, das sei nicht beauftragt.

Wonach fragten Bürger?

Die erste Frage, die mich nach dem 25. Mai 2018 erreichte, war eine Anfrage von mehreren extrem sehschwachen Personen. Sie fragten, ob nicht auch sie ein Recht darauf hätten, über Videoaufzeichnungen im neuen Einkaufszentrum sowie bei einem großen Elektronikmarkt aufgeklärt zu werden, wenn sie dort einkaufen gehen. Der Datenschutzbeauftragte des Einkaufszentrums war kommunikationsbereit. Er teilte uns mit, dass das Einkaufszentrum nur für die Kameras in den Gängen verantwortlich sei und nicht für die Kameras in den Geschäften selbst. Jedes einzelne der über achtzig Geschäfte wäre für die in seinem Bereich hängenden Kameras selbst verantwortlich und müsste auch selbst auf die Videoüberwachung aufmerksam machen. Eine Information für Blinde bzw. Sehschwache wäre derzeit seitens des Einkaufszentrumsmanagements nicht vorgesehen. Wir hakten bei der zuständigen Behörde nach. Die Behörde antwortete recht schnell und ausführlich, hatte aber leider auch noch keine Lösung für das Problem.

Eine Bürgerin wendete sich an uns, weil der Bäcker in ihrer Nachbarschaft Kameras rund um die Bäckerei aufgehängt hat und den Bürgersteig filmt. Sie hatte mit dem Bäckermeister bereits gesprochen, der zeigte sich aber uneinsichtig. Es meldeten sich noch weitere Nachbarn und beschwerten sich über die Kameras an der Bäckerei. Ehe ich mich versah, hatte die Nachbarschaft eine Unterschriftenaktion gegen die Kameras an der Bäckerei organisiert, die sie dann an die Aufsichtsbehörde schicken wollen.

Betroffene bekamen ungewollte Newsletter von einem Erotik-Versand. Gemeinsam mit dem betrieblichen Datenschutzbeauftragten gingen wir der Sache nach, denn eigentlich schickt das Unternehmen nur Newsletter an Kunden, die wirklich den Haken gesetzt haben. Es stellte sich dann heraus, dass die E-Mail-Adressen der Betroffenen durch einen Adresshändler weitergeleitet worden waren, der Verantwortliche darauf vertraut hatte, dass der Adresshändler auch wirklich Einwilligungen von allen Betroffenen hatte, und der Verantwortliche hatte auch keinen Prozess, dass Adressen von Adresshändlern mit Kundendaten verglichen werden, die keine Newsletter wünschen.

Ein Verein, dessen Geschäftsstelle in einem anderen Bundesland ist als laut Satzung der Sitz des Vereins, fragte, bei welcher Behörde er den Datenschutzbeauftragten melden müsse. Ich riet, den Datenschutzbeauftragten in jedem Fall in dem Bundesland zu melden, in dem der Verein laut Satzung den Sitz hat, und dann die Behörde zu fragen, ob es sinnvoll ist den Datenschutzbeauftragten zusätzlich in dem Bundesland zu melden, in dem die Geschäftsstelle ist, da ja auf der Webseite, den Flyern und so weiter die Adresse der Geschäftsstelle steht. Telefonisch wurden sie gebeten, die Anfrage schriftlich einzureichen. Das taten sie im August 2018. Die Behörde antwortete im März 2019, dass die Anfrage eingegangen sei, sie aber so überlastet wären, dass die Beantwortung noch etwas dauern würde.

Seit Herbst häuft sich die Frage: Wie können wir uns gegen Tracking wehren? Was können wir machen, damit das von Webseiten eingesetzte Analyse-Tool uns nicht erfasst?

Warum dürfen wir kein WhatsApp nutzen? Diese Frage erreicht mich bis heute mehrfach. Gibt es nicht doch eine Möglichkeit, dass wir WhatsApp nutzen können?

Fotos und Videos

Es häuften sich auch die Nachfragen zu Einwilligungen für Fotos und Videos insbesondere von Kindern, die dann zu Werbemaßnahmen veröffentlicht werden.

Brauchen wir wirklich die Einwilligung von beiden Eltern? Wie alt muss das Kind sein, um mitzubestimmen? Müssen wir wirklich für jedes Kindergartenfest erneut eine Einwilligung einholen? Dürfen wir Fotos von Kindern aus dem Ausland (Nicht-EU) auch ohne Einwilligung verwenden? Wenn ich als Elternteil ein Gruppenfoto von der Klasse meiner Kinder mache und bei Facebook veröffentliche, dann brauche ich dafür doch keine Einwilligung oder? Müssen wir wirklich für jedes Medium, in dem wir die Fotos veröffentlichen, eine extra Einwilligung haben? Reicht es nicht zu schreiben, wir veröffentlichen die Fotos? Müssen wir wirklich sagen, wir veröffentlichen die Fotos in unseren Flyern, in der lokalen Presse, in sozialen Medien? Wie lange dürfen wir die Fotos verwenden? Brauchen wir wirklich nach zwei Jahren eine erneute Einwilligung, wenn wir die Fotos weiter nutzen wollen? Darf ich wirklich keine Fotos von der Geburtstagsfeier meines Kindes in soziale Netzwerke posten? Ich mach das doch privat und verfolge damit keine geschäftlichen Zwecke.

Auch hier hat sich mit der DSGVO eigentlich nicht viel geändert. Andere, in Deutschland bereits bestehende Gesetze, wurden nicht geändert. Wenn ein Kind nicht fotografiert werden will, dann ist es völlig egal, wie alt das Kind ist. Sagt das Kind Nein, dann ist das Nein zu akzeptieren, egal was die Eltern sagen. Auf Grund der Nein-bleibt-Nein-Gesetze spielt das Alter des Kindes bei einem „Nein“ in der deutschen Rechtsprechung keine Rolle.

Das Bürgerliche Gesetzbuch sagt, dass Kinder im Alter von sieben beschränkt geschäftsfähig sind.

Sagt das Kind „ja“ und einer der Erziehungsberechtigten „nein“, darf das Kind jedoch nicht fotografiert werden, da das „nein“ des Erziehungsberechtigten zum Wohl des Kindes ist. Entsprechend DSGVO könnte ein Kind ab dem Alter von sechzehn Jahren allein bestimmen, ob es fotografiert werden möchte. Sagt einer der Erziehungsberechtigten jedoch „nein“ bleibt es ein Fall für die Gerichte, ob hier nicht doch das Erziehungsrecht zum Wohl des Kindes überwiegt. Das zeigt schon, dass Fotos von Kindern zu veröffentlichen ein ziemlich kompliziertes Thema ist.

Das Problem mit der Einwilligung aller Erziehungsberechtigten kennt die Medizin nur zu gut. Bei Fotos und Videos ist das nicht anders. Hier kann der Verantwortliche schnell zum Spielball im Scheidungskrieg werden, wenn nur ein Elternteil eingewilligt hat. In der Medizin gibt es mittlerweile Rechtsprechungen, wann die Einwilligung eines Elternteils ausreichend ist und wann nicht. Das ist aber nicht auf Fotos und Videos zu übertragen. Es ist in jedem Fall ratsam, stets die Einwilligung aller Erziehungsberechtigten einzuholen.

Selbstverständlich sind auch Einwilligung für Fotos und Videos zweckgebunden. Der Zweck muss genau angegeben werden. Eine Generaleinwilligung für alle Kindergarten- und Schulveranstaltungen im Laufe des Leben des Kindes gibt es nicht.

Was ist mit Veranstaltungen wie Parteitagen, Mitgliederversammlungen, Preisverleihungen oder ähnliches? Auch hier hat sich nichts geändert. Die einfachste Lösung ist hier nach wie vor, wenn nicht nur die Bühne abgelichtet werden soll und freie Platzwahl herrscht, die Flächen, die fotografiert werden, zu markieren und bekannt zu geben. Alle Besuchenden müssen die Information erhalten, wo sie sich aufhalten können, wenn sie nicht fotografiert werden möchten.

Was ist mit Konferenzen? Auch hier hat sich nichts geändert. Werden die Vortragenden für ein Streaming aufgezeichnet oder werden Fotos gemacht, benötigt der Veranstalter die Einwilligung des jeweiligen Vortragenden. Auch wenn die Konferenz in Brüssel ist? Ja, die DSGVO gilt für die gesamte EU.

Zum Thema Video wurde natürlich auch immer wieder nachgefragt: Lässt sich wirklich nichts gegen die Kameras in den U- und S-Bahnen machen? Wieso sind keine Schilder an U-Bahnstationen, die auf die Überwachung hinweisen?

Beschäftigte, Freiheitsstrafen und Einwilligungen

Mehrfach erreichte mich die Anfrage von Verantwortlichen: „Unser Betriebsrat lässt nicht zu, dass die Beschäftigten die Verpflichtung auf Vertraulichkeit unterschreiben.“ Auf die Frage nach dem Warum bekam ich die Antwort: „Weil da drin steht, dass die Mitarbeiter ins Gefängnis kommen können.“ In einem Fall hatten die Beschäftigten sogar mit Einverständnis des Betriebsrats bei ihrer Einstellung die Verpflichtung auf das Datengeheimnis unterschrieben.

Ein Verantwortlicher hatte die zuständige Behörde gefragt und zur Antwort bekommen: „Generell ist hierzu anzumerken, dass eine zur Vertraulichkeit verpflichtende Tätigkeit die Unterzeichnung einer entsprechenden Verpflichtungserklärung voraussetzt.“

Gibt es nicht doch eine Möglichkeit, dass ich Fotos meiner Beschäftigten veröffentliche? Die Veröffentlichung von Fotos würde einer Einwilligung bedürfen. Eine Einwilligung muss freiwillig sein. Bei Beschäftigten im abhängigen Beschäftigungsverhältnis ist das mit der Freiwilligkeit schwierig. Eine Veröffentlichung von abgelichteten Beschäftigten sollte daher unterlassen werden. Was anderes ist es bei leitenden Angestellten. Allerdings sind Führungskräfte nicht zwingend leitende Angestellte. §5 Abs. 3 und Abs. 4 BetrVG definiert, wann Beschäftigte leitende Angestellte sind.

Spam Beschwerdestelle

Ich persönlich bekam dreimal im vergangenen Jahr von der Spam-Beschwerdestelle eine Mitteilung, dass bei der Überprüfung meines Spams herauskam, ich hätte angeblich ca. sechs Monate zuvor mit einer bestimmten IPv4-Adresse an einem Gewinnspiel teilgenommen und zu einer sekundengenauen Uhrzeit in die Weiterleitung meiner Daten eingewilligt. Es wurde ein Link zu dem Gewinnspiel angegeben. Auch in der Beratung häuften sich derartige Berichte anderer Betroffener. Es ist hier nicht gerade einfach, einen Gegenbeweis zu liefern. Ich selbst hatte Glück. Da ich bei einem Anbieter bin, der den einzelnen Haushalten nur IPv6-Adressen gibt und dann hunderten IPv6-Adressen dieselbe IPv4-Adresse, ist die IPv4-Adresse hier zur Identifizierung nicht ausreichend. Zudem sollte ich angeblich Microsoft-Produkte für die Teilnahme am Gewinnspiel genutzt haben. In meinem Haushalt gibt es gar keine Microsoft-Produkte.

Es ist aber schwer, den Betrug nachzuweisen, denn die wenigsten haben so viel Ahnung von ihren Routern und Anschlüssen, dass sie angebliche IP-Adressen prüfen könnten. Abgesehen davon, dass die Router die zugeteilten IP-Adressen ja auch nicht sechs Monate und länger speichern.

Die Spam-Beschwerdestelle macht meiner Erfahrung nach einen super Job. Leider ist es ein Kampf gegen Windmühlen. Aber, es lohnt sich.

Amazon und Google

Google hat am 2. April 2019 die Bereitstellung von Google Plus für Privatnutzer abgeschaltet. Google Plus gibt es jetzt nur noch Business to Business (B2B).

Amazon stellt konsequent nur noch Rechnungen an juristische Personen aus. Dadurch entfällt die zehnjährige Aufbewahrungspflicht auf Grund des Steuerrechts für die Anschrift von Privathaushalten. Meines Wissens handelt Amazon nicht mit Waren, die unter §14 Abs. 2 lit. 1 UStG fallen würden.

Fazit:

Die DSGVO hat wesentlich mehr Menschen für das Thema informationelle Selbstbestimmung sensibilisiert. Die meisten Behörden haben aufgestockt und erstaunlich schnell reagiert. WhatsApp und Fotos von Kindern sind vielen wichtig. Verantwortliche sind aufgewacht. Das Thema Datenschutz wird durchaus ernst genommen.

Riko Pieper

Kuriositäten in der [Datenschutz-]Gesetzgebung – Folge 2

Einleitung

Im DANA Heft 3/2017[1] gab es den ersten Artikel über „Kuriositäten in der [Datenschutz-]Gesetzgebung". Damals bezogen sich manche Beispiele noch auf das alte BDSG, andere bereits auf die DSGVO und teilweise auch auf das neue BDSG[2] – letztere waren zu diesem Zeitpunkt noch nicht wirksam.

Nachdem inzwischen gut 1½ Jahre vergangen sind und seit über einem Jahr auch mit der neuen Gesetzgebung gearbeitet werden kann, ist der Autor auf weitere Beispiele gestoßen, die geeignet sind einen zweiten Teil dieser Kuriositätenreihe zu verfassen. Und wer weiß? Eventuell kommen weitere Folgen dazu – das Datenschutzrecht ist ja diesbezüglich sehr ergiebig. Falls den Lesern selbst vergleichbare Kuriositäten aufgefallen sind, teilen Sie uns diese gern per E-Mail mit an: dvd@datenschutzverein.de – Stichwort: „Kuriositäten".

Wie im ersten Artikel sind die Beispiele wieder in drei Kategorien aufgeteilt, wobei es die Kategorie „Toter Code" jetzt nicht mehr gibt, dafür aber die neue „Konflikte zwischen DSGVO und BDSG":

1. Begriffe / Definitionen
2. Konflikte zwischen DSGVO und BDSG
3. Sprachwirrwarr

Die folgenden Ausführungen stellen (wie im ersten Artikel) Beispiele aus der DS-Gesetzgebung dar (hauptsächlich aus der DSGVO und dem BDSG – aber teilweise auch nur aus deren falscher Anwendung – siehe Beispiel 10). Offensichtliche Tipp- oder Übersetzungsfehler, von denen es auch einige gibt und noch mehr gab, werden hier nicht thematisiert.

Manche der folgenden Beispiele sind Aktualisierungen oder Ergänzungen zu Beispielen, die bereits im ersten Artikel behandelt wurden. In diesen Fällen gibt es keine Wiederholungen, sondern es werden ergänzende Aspekte dieser Beispiele erläutert, die aber auch ohne Rückgriff auf den alten Artikel gelesen werden können.

Wie im ersten Artikel wurden die Beispiele aus der speziellen Sicht des Autors formuliert, der als Datenschützer in seiner Rolle als Informatiker und Nicht-Jurist an einer öffentlichen Stelle tätig ist.

Teil I: Begriffe / Definitionen

1. Beispiel: „privacy by design" und „privacy by default"

In der Fachliteratur ist, wenn es um den Art. 25 DSGVO geht, meistens von „privacy by design" und „privacy by default" die Rede. Selbst in Artikeln in deutscher Sprache werden diese Begriffe oft benutzt. Die DSGVO enthält diese Begriffe jedoch nicht – weder in der deutschen, noch in der englischen[3] Version. In der englischen Version wird statt „privacy" der Begriff „data protection" benutzt. Der Art. 25 DSGVO hat die Überschrift: „Data protection by design and by default".

Der englische Begriff „data protection" ist jedoch nicht identisch mit dem amerikanischen „privacy". Dass es in den USA (vorsichtig ausgedrückt) ein anderes Verständnis zum Datenschutz gibt als in Europa, ist bekannt. „Privacy" bezieht sich nur auf die „Privatsphäre"[4] und nicht auf alle personenbezogenen Daten. Das ist ein großer Unterschied. Beispielsweise fallen personenbezogene Daten von Beschäftigten nicht unter „privacy", denn die Daten von Beschäftigten werden im Unternehmenskontext nicht als „Privatsphäre" betrachtet.

Die übliche Sprechweise von „privacy" ist übrigens nicht die englische (Lautschrift: „prɪvəsi" – das „i" wie ein deutsches „i" gesprochen), sondern die amerikanische (Lautschrift: „praɪvəsi" – das „i" wie „ai" gesprochen). Ist es nun nur als konsequent oder als verräterisch zu betrachten, dass sich für den Begriff „Datenschutz" der europäischen DSGVO ein amerikanischer Begriff und sogar die amerikanische Sprechweise dafür durchgesetzt hat, obwohl es in der DSGVO anders (korrekt) steht?

Zugegeben: Das Wort „privacy" geht leichter über die Lippen, als der sperrige Begriff „data protection". Das kann aber nicht der ganze Grund für den Austausch der Begriffe sein. Vielmehr scheint es ein Hinweis darauf zu sein, wie viel Einfluss welche Lobbyisten in wessen Auftrag während der Verhandlungen der DSGVO hatten. Man muss sich nur einmal vorstellen, wie leicht hier Verwirrung gestiftet wird, wenn man sich mit Juristen amerikanischer Unternehmen über die Rechte von Beschäftigten austauscht und dann immer (deren) Begriff „privacy" nutzt, aber den europäischen Datenschutz meint.

Zusätzlich zum Begriff „privacy" kann man sich auch die beiden anderen (wirklich in der englischen Version vorhandenen) Begriffe des Art. 25 DSGVO „design" und „default" bzw. deren deutsche Übersetzung einmal näher betrachten. Gegen den Begriff „Voreinstellungen" wäre als Übersetzung von „default" nichts zu sagen. Übersetzt wird „default" aber mit „datenschutzrechtliche Voreinstellungen". Das ist im Kontext der DSGVO sicher nicht ganz verkehrt, aber es ist nicht Sache der Übersetzer, in den Übersetzungen etwas zu ergänzen, was im Original nicht steht. Gerade bei diesem Text, bei dem jedes Wort lange verhandelt wurde, können dadurch leicht Missverständnisse oder sogar Fehler entstehen. Spätestens bei dem anderen Begriff „design" ist diese Ergänzung problematisch, denn er wird mit „Technikgestaltung" übersetzt statt nur mit „Gestaltung". Inhaltlich wird der Artikel dann auch korrekt übersetzt, indem gleich im Absatz 1 Satz 1 von „technischen und organisatorischen Maßnahmen" die Rede ist. Das „design" beschränkt sich also absolut nicht nur auf technische Aspekte, wie es die deutsche Übersetzung des Titels vermuten lässt.

Eine allgemeine Vorgabe für die Übersetzer in Bezug auf (klarstellende) Er-

gänzungen scheint es nicht zu geben, denn beispielsweise die spanische Version des Titels von Art. 25 DSGVO lautet: „Protección de datos desde el diseño y por defecto“ – eine wörtliche Übersetzung der englischen Version.

Um einen Übersetzungsfehler kann es sich bei den Ergänzungen in der deutschen Version kaum handeln, aber was ist dann die Ursache? Ein namhafter Professor, der nicht nur Vorlesungen zum Internet-, IT- und Datenschutzrecht für seine Studenten hält, sondern auch Seminare für Anwälte und Datenschutzbeauftragte, hat dazu seine eigene Theorie: Von ihm ist die Vermutung zu hören, dass es sich bei den Übersetzern der DSGVO nicht wirklich um Übersetzer gehandelt haben kann, sondern dass die damit Betrauten beispielsweise aus dem Bereich der Schweinezucht kommen könnten.

2. Beispiel: „öffentliche“ oder „nichtöffentliche“ Stelle – das ist hier die Frage

In der DSGVO wird (nicht so grundsätzlich wie im alten BDSG mit eigenen Abschnitten – aber doch oft) zwischen öffentlichen und nichtöffentlichen Stellen unterschieden. Eine Definition für öffentliche oder nichtöffentliche Stellen gibt es in der DSGVO jedoch nicht. Das blieb den nationalen Gesetzgebern überlassen. Im BDSG (alt wie neu) gibt es dann die entsprechende Klarstellung im § 2. Ministerien und Ämter sind danach öffentliche Stellen, die privatrechtlichen Stellen sind nichtöffentlich – bis hierhin scheint alles klar zu sein.

Dann kommt jedoch eine wichtige Ergänzung im § 2 Abs. 4 Satz 2:

„Nimmt eine nichtöffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.“

Dieser Fall betrifft nur sehr wenige Unternehmen, sodass über diese spezielle Konstellation wenig in der Literatur zu finden ist.

Aufgrund der Tatsache, dass es ja um die Bestimmung geht, ob man eine öffentliche oder eine nichtöffentliche Stelle ist, ist es ungünstig, dass der Satz als Voraussetzung bereits die nichtöffentliche Stelle enthält. Die Definition ist somit rekursiv, da sie sich selbst enthält[6].

Würde man das Wort „nichtöffentliche“ streichen, dann hätte man keinen Selbstbezug mehr, sondern eine klare Aussage (die vermutlich auch so gemeint war):

„Nimmt eine ~~nichtöffentliche~~ Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.“

Die Beschränkung der Aussage auf nichtöffentliche Stellen ist also überflüssig und schafft erst das Problem, dass man sich beim dritten Wort des Satzes Gedanken machen muss, ob das nun für die eigene Stelle gilt oder nicht.

Darüber hinaus gibt es aber auch noch den § 2 Abs. 5 Satz 1[7]:

„Öffentliche Stellen des Bundes gelten als nichtöffentliche Stellen im Sinne dieses Gesetzes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.“

Auch dieser Satz enthält wieder die festzustellende Aussage als Voraussetzung (in diesem Fall „öffentliche Stellen des Bundes“) in sich, sodass es wieder ein selbstbezüglicher Satz ist. Damit schließt sich der Kreis, falls man sowohl eine hoheitliche Aufgabe (des Bundes) wahrnimmt als auch „als öffentlich-rechtliches Unternehmen am Wettbewerb“ teilnimmt. Jetzt kommt es bei der Frage, ob man öffentliche oder nichtöffentliche Stelle ist, darauf an, in welcher Reihenfolge man die beiden Aussagen liest.

Die Situation erinnert an „unbestimmte Ausdrücke“[8] in der Mathematik, bei denen das konkrete Ergebnis vom Einzelfall abhängt. Unbestimmte Ausdrücke sind:

$0:0$, $0 \cdot \infty$, $\infty - \infty$, $\infty:\infty$, 0^0, ∞^0 und 1^∞

Ein Beispiel, das zu einem Ausdruck der Form 1^∞ führt, ist die Definition der Eulerschen Zahl „e“[9]:

$$e = \lim_{n \to \infty} \left(1 + \frac{1}{n}\right)^n$$

Der Ausdruck $\lim_{n \to \infty}$ bedeutet, dass der Wert von „n“ sehr, sehr groß angenommen wird – also gegen unendlich geht. Einerseits ist 1[10] beliebig oft mit sich selbst multipliziert immer 1 und andererseits ist jede beliebige Zahl, die größer als 1 ist[11] unendlich oft mit sich selbst multipliziert immer unendlich groß. Nach der einen Regel kommt also als Ergebnis immer 1 heraus, nach der anderen immer unendlich.

Das Ergebnis dieses konkreten Ausdrucks wird als „Eulersche Zahl“ oder kurz „e“ bezeichnet und ist ungefähr: 2,7182818. Man kann leicht mit einem Taschenrechner überprüfen, dass sich das Ergebnis für große Werte von „n“ diesem Wert nähert.

Es wäre schön, wenn es bei dem oben beschriebenen Problem zur Bestimmung einer öffentlichen oder nichtöffentlichen Stelle ähnliche Möglichkeiten gäbe sich dem Ergebnis wenigstens anzunähern.

3. Beispiel: Noch'n Begriff[12]: „Behörde“

Die im BDSG vorhandene Definition von öffentlichen Stellen unterscheidet nur zwischen öffentlichen Stellen des Bundes und öffentlichen Stellen der Länder. Es gibt aber öffentliche Stellen (Behörden), die weder zum Bund noch zu den Ländern gehören. Europäische Behörden wie z. B. die europäische Luftfahrtbehörde EUROCONTROL[13] bezeichnen sich als öffentliche europäische Stellen. Für diese Stellen selbst gelten statt der DSGVO andere Vorgaben, aber sie selbst bezeichnen sich als öffentliche Stellen (und Behörden) im Sinne der DSGVO. Wenn nun eine deutsche öffentliche Stelle personenbezogene Daten an eine solche europäische öffentliche Stelle (Behörde) übermittelt, dann müsste als Rechtsgrundlage für die Übermittlung der § 25 Abs. 1 BDSG (Datenübermittlungen durch öffentliche Stellen – an öffentliche Stellen) herangezogen werden können. Die Frage ist nur: Woraus lässt sich ableiten, dass solche EU-Institutionen „öffentliche Stellen“ im Sinne der DSGVO sind? Eine Definition für eine europäische öffentliche Stelle findet sich weder in der DSGVO noch im BDSG.

Ähnlich wie die Begriffe „öffentliche“ oder „nichtöffentliche Stelle“ ist auch der Begriff „Behörde“ nicht in der DSGVO definiert, obwohl er durchaus benutzt wird. Im Gegensatz zur öffentlichen oder nichtöffentlichen Stelle ist der Begriff der Behörde jedoch auch im BDSG nicht definiert.

Im alten BDSG gab es die Möglichkeit der Verarbeitung personenbezogener Daten im § 28 Abs. 1 für „eigene Geschäftszwecke“[14], die jedoch auf die nicht-öffentlichen[15] Stellen beschränkt war (weil § 28 im Teil 3 für nicht-öffentliche Stellen stand). In der DSGVO scheint es diese Beschränkung nicht mehr für alle öffentlichen Stellen zu geben, sondern nur noch für Behörden, denn jetzt steht im Art. 6 DSGVO (Rechtmäßigkeit der Verarbeitung) am Ende von Abs. 1:

„Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.“

Buchstabe f ist der Fall der Verarbeitung „zur Wahrung der berechtigten Interessen des Verantwortlichen…“.

Das bedeutet, dass Behörden keine „berechtigten Interessen“ haben, die nicht auf einer klaren gesetzlichen Vorgabe oder Einwilligung beruhen, sodass diese als Rechtsgrundlage immer eine der Optionen von Art. 6 Abs. 1 lit a – e DSGVO brauchen.

Hier stellt sich nun die Frage, ob der (europäische) Gesetzgeber diese Einschränkung bewusst nur für (richtige) Behörden aufrechterhalten wollte und nicht für alle öffentlichen Stellen wie z. B. die eigentlich nichtöffentlichen Stellen, die nur aufgrund ihrer hoheitlichen Aufgabe öffentliche Stellen sind (siehe Beispiel 2). Soviel steht jedenfalls fest: Um einen Übersetzungsfehler handelt es sich nicht. In der DSGVO wird im englischen Original häufig zwischen „public body“ und „public authority“ unterschieden, welche konsistent in „öffentliche Stelle“ und „Behörde“ übersetzt wurden.

Nachdem weder DSGVO noch BDSG hier weiterhelfen, muss man sich an anderer Stelle nach einer Definition erkundigen. Von Juristen hört man in diesem Zusammenhang (mal wieder): „Es kommt darauf an“. Dann wird argumentiert, dass man bei der Ausübung einer hoheitlichen Aufgabe eine Behörde ist, bei anderen Verarbeitungen, die sich nicht aus der hoheitlichen Aufgabe ableiten lassen, jedoch nicht. Das mag korrekt sein, hilft im konkreten Beispiel aber nicht viel weiter, denn wenn die Frage, ob eine verantwortliche Stelle nun eine Behörde ist oder nicht, davon abhängt, ob die Verarbeitung zur Erfüllung der hoheitlichen Aufgabe erforderlich ist, dann ist man automatisch eine Behörde, wenn man eine öffentliche Stelle (aufgrund der hoheitlichen Aufgabe) ist. Die Unterscheidung zwischen Behörden und öffentlichen Stellen wäre dann überflüssig.

Im Ergebnis stellt sich die Situation folgendermaßen dar:

Wenn man als öffentliche Stelle personenbezogene Daten im Rahmen der hoheitlichen Aufgabe verarbeitet, dann hat man eine klare Rechtsgrundlage (vermutlich Art. 6 Abs. 1 lit c oder e DSGVO).

Wenn man personenbezogene Daten verarbeitet, die nicht zur Umsetzung der hoheitlichen Aufgabe erforderlich sind, dann ist man keine Behörde und kann sich somit auf Art. 6 Abs. 1 lit f DSGVO als Rechtsgrundlage berufen.

Es fällt schwer zu glauben, dass dies die Intention des Gesetzgebers war, denn die Einschränkung im letzten Satz von Art. 6 Abs. 1 DSGVO wäre dann völlig sinnfrei – aber man kann damit arbeiten.

Teil II: Konflikte zwischen DSGVO und BDSG

4. Beispiel: „Videoüberwachung“

Die Videoüberwachung kommt in der DSGVO gar nicht konkret vor. Es gibt jedoch Stellen[16], an denen die „Überwachung“ genannt ist und das kann dann auch die Videoüberwachung einschließen, sodass die Videoüberwachung nicht gänzlich im Widerspruch zur DSGVO sein kann.

Mit § 4 BDSG (Videoüberwachung öffentlich zugänglicher Räume) gibt es jedoch einen konkreten Paragraphen, der die Videoüberwachung erlaubt. Für öffentliche Stellen gibt es wohl auch hinreichende Öffnungsklauseln in der DSGVO, aus denen sich der § 4 BDSG herleiten lässt. Von mehreren Vertretern deutscher Aufsichtsbehörden wird jedoch entschieden bestritten, dass es auch für nichtöffentliche Stellen entsprechende Öffnungsklauseln gibt. Die Anwendbarkeit der Begründung im § 4 BDSG, wonach die Videoüberwachung von „öffentlich zugänglichen großflächigen Anlagen…“ dem „Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen“ dient und somit „als ein besonders wichtiges Interesse“ anzusehen ist, wird im Falle einer nichtöffentlichen Stelle seitens der Vertreter der Aufsichtsbehörden bestritten – das sei Aufgabe der Polizei oder anderer öffentlicher Stellen.

Die Vertreter dieser Aufsichtsbehörden haben auch angekündigt, gegen Stellen vorzugehen, die sich unter Berufung auf das oben genannte öffentliche Interesse auf eine Videoüberwachung nach § 4 BDSG als Rechtsgrundlage berufen. Die eigentliche Rechtsgrundlage (auf oberster Ebene) muss ja sowieso eine der sechs Optionen aus Art. 6 Abs. 1 DSGVO (Rechtmäßigkeit der Verarbeitung) sein. Aber welche soll es sein?

a Wenn eine (wirksame) Einwilligung vorliegt, ist dies eine wirksame Rechtsgrundlage. Das ist aber für Prozesse schwierig bis unmöglich, die mit allen betroffenen Personen funktionieren müssen, weil die Einwilligung immer freiwillig sein muss und auch jederzeit widerrufen werden kann. Darüber hinaus muss bei der Einwilligung auch auf dieses Widerrufsrecht hingewiesen werden.

b Die Erfüllung eines Vertrages kann eine Rechtsgrundlage sein, aber die Videoüberwachung muss dann auch zur Erfüllung des Vertrages „erforderlich“ sein. Das ist ein eher untypisches Beispiel für die Videoüberwachung.

c Wenn die Videoüberwachung zur Erfüllung einer rechtlichen Verpflichtung „erforderlich“ ist, wäre diese Option einschlägig. Es muss sich aber wirklich um eine „Verpflichtung“ handeln und die Videoüberwachung muss auch „erforderlich“ sein. Auch diese Voraussetzungen sind für die Videoüberwachung eher untypisch. Der oben genannte § 4 BDSG verpflichtet nicht zur Videoüberwachung, sondern erlaubt sie nur unter den genannten Voraussetzungen, sodass er nicht als Rechtsgrundlage in diesem Sinne dienen kann.

d Wenn die Verarbeitung „erforderlich“ ist, um lebenswichtige Interessen der betroffenen Person oder einer ande-

ren natürlichen Person zu schützen, kann dies als Rechtsgrundlage herangezogen werden. Wie bei den zuvor genannten Optionen ist das wohl eher ein untypischer Fall für eine Videoüberwachung.

e Wenn die Videoüberwachung für die Wahrnehmung einer Aufgabe im öffentlichen Interesse liegt und hierzu „erforderlich" ist, kann diese Option eine Rechtsgrundlage sein. Die Erforderlichkeit wird hier in den meisten Fällen schwer zu begründen sein und außerdem gibt es gegen diese Option ein Widerspruchsrecht[17] seitens der betroffenen Person, auf das diese auch hingewiesen[18] werden muss.

f Die „berechtigten Interessen" des Verantwortlichen sind der letzte Notnagel und auch die schwächste der hier genannten Rechtsgrundlagen, weshalb auch (wie bei lit e – siehe oben) sowohl das Widerspruchsrecht als auch die Informationspflicht bezüglich des Widerspruchsrechts gelten. Darüber hinaus müssen die betroffenen Personen bei dieser Option auch noch über die (angenommenen/behaupteten) „berechtigten Interessen" des Verantwortlichen explizit informiert[19] werden.

In der Praxis wird es bei nichtöffentlichen Stellen wohl meistens auf den Buchstaben „f" hinauslaufen – mit allen damit verbundenen Problemen. Eine klare Rechtsgrundlage ohne Widerspruchsrecht (lit c) kommt wohl nur bei (einigen) öffentlichen Stellen in Betracht.

Unabhängig von der Rechtmäßigkeit an sich gibt es auch noch den Konflikt zwischen dem Art. 13 DSGVO und den im § 4 BDSG angegebenen Informationspflichten. Im Abs. 2 steht dort, dass der „Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen ... durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen" sind. Das ist deutlich weniger, als der Art. 13 DSGVO verlangt.

Im § 4 Abs. 4 BDSG steht dann zwar, dass auch die Art. 13 und 14 DSGVO gelten, aber nur unter der Voraussetzung, dass die Videos einer „bestimmten Person zugeordnet" werden. Die zusätzliche Angabe einer URL oder eines QR-Codes auf einem Informationsschild, über die man die restlichen Informationen des Art. 13 DSGVO abrufen kann, wären für den Verantwortlichen durchaus zumutbar (fair[20]). Eine Öffnungsklausel, über die die Informationspflichten derart eingeschränkt werden, lässt sich in der DSGVO nicht finden.

Insgesamt ist die hier beschriebene Situation nicht mehr kurios, wie es der Titel dieses Beitrags suggeriert, sondern schlicht eine Frechheit gegenüber den Verantwortlichen und deren Datenschutzbeauftragten. Es handelt sich schließlich nicht um einen Tippfehler oder eine anders entstandene Unklarheit oder Lücke im Gesetz, sondern um eine bewusste Überschreitung der Kompetenz des deutschen Gesetzgebers – speziell des Innenministeriums und hier speziell des ehemaligen Innenministers Thomas de Maizière – gegen die auch sofort Vertragsverletzungsverfahren angekündigt wurden. Diskutiert wurde darüber vor der Verabschiedung des Gesetzes genug[21], sodass keiner (der Beteiligten am Gesetzgebungsprozess) sagen kann, er hätte davon nichts gewusst. Dass eine EU-Verordnung das Maß der Dinge ist – und nicht das BDSG – steht klar im Art. 288 AEUV[22], hat sich aber offenbar noch nicht in allen Ministerien herumgesprochen. Dort steht: „Die Verordnung hat allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat."

Eine empfehlenswerte Lektüre in diesem Zusammenhang ist auch die „Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24. Februar 2016 im Ausschuss Digitale Agenda des Deutschen Bundestags"[23] – Antworten von Prof. Rossnagel auf Fragen der Bundestagsabgeordneten zur DSGVO (siehe insbesondere die Absätze 3 und 4 von Antwort 2). Dort steht bezüglich der Situation, dass sich EU-Verordnung und nationales Recht widersprechen:

„Dieses Nebeneinander kann dazu führen, dass sich Regelungen widersprechen und sich die Frage stellt, welche Regelung anwendbar ist. In einem solchen Konflikt genießt die Unionsverordnung Anwendungsvorrang. Sie ist von den nationalen Behörden und Gerichten anzuwenden. Die konfliktierende – weiterhin geltende – deutsche Vorschrift darf in diesem konkreten Konfliktfall nicht angewendet werden – gleichgültig, ob sie früher oder später als die Unionsnorm ergangen ist. Dieser Anwendungsvorrang, den sowohl der Europäische Gerichtshof als auch das Bundesverfassungsgericht ihrer Rechtsprechung zugrunde gelegt haben, wurde auch in der Protokollerklärung Nr. 17 zum Vertrag von Lissabon anerkannt."

Das bedeutet, dass die DS-Aufsichtsbehörden diesbezüglich nicht erst ein oberstes Gerichtsurteil abwarten müssen, sondern dass sie bereits jetzt im Konfliktfall nur die DSGVO zu beachten haben, und sie haben angekündigt sich daran zu halten.

5. Beispiel: Log-Dateien und weitere allgemeine zur Aufrechterhaltung des Betriebs erforderliche Verarbeitungen

Im BDSG-alt gab es für nicht-öffentliche Stellen folgenden § 31 „Besondere Zweckbindung":

„Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden."

Für öffentliche Stellen gab es im § 14 Abs. 4 BDSG-alt einen gleichlautenden Absatz.

In der DSGVO gibt es keinen entsprechenden Artikel aber im neuen BDSG gibt es im § 23 „Verarbeitung zu anderen Zwecken durch öffentliche Stellen" Abs. 1 Nr. 6 folgende erlaubte Ausnahme für Verarbeitungen, die nicht dem ursprünglichen Zweck der Verarbeitung entsprechen:

Wenn „sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen."

Im anschließenden § 24 BDSG ist keine entsprechende Ausnahme für nichtöffentliche Stellen genannt, sodass nun in Kreisen von Datenschützern teilweise angenommen wird, dass es bei nichtöffentlichen Stellen keine Rechtsgrundlage mehr für das Anlegen von Log-Dateien oder anderen zur „Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen“ erforderlichen Verarbeitungen mehr gibt.

Das ist aus Sicht des Autors eine falsche Annahme. Man muss aber leider um mehrere Ecken denken, bis man zur Auflösung kommt.

Zum einen muss man feststellen, dass die oben genannten §§ des alten BDSG gar keine Erlaubnis enthielten, sondern nur Beschränkungen! Die eigentliche Erlaubnis stand auch im alten Gesetz nicht explizit, sondern wurde implizit (weil erforderlich) vorausgesetzt. Sie ergab sich beispielsweise aus der Vorgabe der technischen und organisatorischen Maßnahmen, zu denen auch Log-Dateien etc. gehören. Zum anderen waren die Paragrafen bzw. der Absatz im alten BDSG nur deklaratorisch (und somit überflüssig), denn bei einer Verarbeitung dieser Daten für einen anderen Zweck hätte man dafür keine Rechtsgrundlage, sodass es dieser zusätzlichen Beschränkung eigentlich gar nicht bedurfte.

Das ist der Grund dafür, dass die DSGVO diese Sonderfälle nicht explizit behandelt, und es ist aus EU-Sicht auch keine Veränderung, denn die alte EU DS-Richtlinie enthielt diesbezüglich auch keine Angaben. Das wurde nur im deutschen BDSG ergänzt und nun fällt es auf, wenn diese Klarstellung (teilweise) fehlt. Da es aber nur für öffentliche Stellen hinreichenden Spielraum (Öffnungsklauseln) für so eine Klarstellung gibt, ist sie auch nur in diesem Fall angegeben und im nichtöffentlichen nicht.

Wenn man nun diesen Hintergrund nicht kennt (oder beim Lesen des BDSG nicht daran denkt), dann ist die Gegenüberstellung der beiden §§ 23 und 24 tatsächlich sehr missverständlich und der § 23 Abs. 1 Nr. 6 alles andere als eine Klarstellung, sondern eher die Ursache für das hier dargestellte Missverständnis.

Leider gibt es weitere Fälle solcher missverständlichen „Klarstellungen“, die nur mit ähnlicher Argumentation wie in dem hier dargestellten Fall aufgelöst werden können. Als Beispiel seien hier die Aufgaben des DSB genannt, die im § 7 BDSG für öffentliche Stellen ausführlich (fast identisch zur DSGVO) und im § 38 BDSG für nichtöffentliche Stellen gar nicht beschrieben sind.

6. Beispiel: Gilt die DSGVO auch für Ergänzungen im BDSG

In der zweiten Jahreshälfte 2018 gab es Diskussionen darüber, ob die im § 38 BDSG enthaltene erweiterte[24] Pflicht zur Benennung eines Datenschutzbeauftragten (DSB) von nichtöffentlichen Stellen aufrecht erhalten bleiben oder ob sie aus dem BDSG wieder gestrichen werden sollte. Eine Öffnungsklausel für diese Ergänzung im BDSG gibt es ausdrücklich im Art. 37 Abs. 4 DSGVO. Sie wurde auf besonderen Druck der deutschen Verhandlungspartner dort aufgenommen. Umso mehr verwunderte ein Vorschlag auf Initiative der Länder Bayern und Baden-Württemberg, dass das neue BDSG ausgerechnet in diesem Punkt wieder geändert und auf diese zusätzliche Benennungspflicht verzichtet werden sollte. Der Vorschlag fand dann zwar im Bundesrat keine Mehrheit und anschließend auch im Bundestag nicht, aber die Lobbyisten hatten es immerhin geschafft, dies Thema so weit zu bringen.

An dieser Stelle sei auch einmal daran erinnert, dass das Konzept der unternehmensinternen Kontrolle durch eigene DSB vor Jahrzehnten auf Wunsch der Wirtschaft ins deutsche BDSG aufgenommen wurde, weil man einerseits kaum eine Möglichkeit sah, die im BDSG vorgesehenen Aufgaben ohne (ausgebildete) DSB umzusetzen und sich andererseits so erhoffte, von den Aufsichtsbehörden (AB) ein Stückweit in Ruhe gelassen zu werden. Für letzteres gab es im BDSG sogar einen zusätzlichen Anreiz zur Bestellung eines DSB, denn wer einen DSB bestellt hatte, war von der Meldepflicht (des Verfahrensverzeichnisses an die eigene Aufsichtsbehörde) nach § 4d Abs. 2 BDSG-alt befreit. Einen entsprechenden zusätzlichen Anreiz gibt es in der DSGVO und im aktuellen BDSG leider nicht, was ggf. eine Ursache für die oben genannte Initiative war.

Das Kuriose an dieser Geschichte ist nun, wie in diesem Zusammenhang für oder gegen die Streichung der Bestellpflicht argumentiert wurde und hier insbesondere der „Kompromiss“, der von einigen Datenschützern ins Spiel gebracht wurde:

Dort wurde argumentiert, dass die im BDSG enthaltene erweiterte Pflicht zur Benennung eines DSB problemlos erhalten bleiben kann, weil ein Verstoß dagegen nicht sanktioniert werden kann. Die Argumentationskette ging in etwa wie folgt:

Ein Verstoß gegen die DSGVO liegt nicht vor, weil die erweiterte Pflicht zur Benennung des DSB nicht in der DSGVO steht, sondern nur im BDSG. Somit greift der Art. 83 DSGVO (Allgemeine Bedingungen für die Verhängung von Geldbußen) nicht und das BDSG enthält keine eigene Sanktion gegen einen Verstoß gegen § 38.

Das sieht nach einer gelungenen Win-Win-Situation aus. Die Befürworter der erweiterten Benennungspflicht sind zufrieden, weil § 38 BDSG unverändert bleiben kann und die Gegner sind zufrieden, weil sie diesen Paragraphen problemlos ignorieren können.

Wenn man aber anfängt so zu argumentieren, dann stellen sich weitere Fragen wie z. B.:

- Wie sieht es mit einem Verstoß gegen die (sowieso gegenüber der DSGVO schon eingeschränkte) Informationspflicht im Falle einer Videoüberwachung nach § 4 BDSG[25] aus?
- Wird auch ein Verstoß gegen § 26 BDSG (Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses) nicht sanktioniert?

Teil III: Sprachwirrwarr

7. Beispiel: Braucht man für die Verarbeitung besonderer Kategorien personenbezogener Daten keine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO?

Einerseits enthält Art. 6 Abs. 1 DSGVO eine **vollständige Aufzählung** (lit a bis lit f) von Optionen, von denen mindes-

tens eine erfüllt sein muss, damit eine Verarbeitung personenbezogener Daten rechtmäßig ist.

Andererseits enthält Art. 9 DSGVO für die „Verarbeitung besonderer Kategorien personenbezogener Daten" eigene Voraussetzungen.

Nun wird von vielen Juristen die Meinung vertreten, dass diese beiden Artikel gleichberechtigt nebeneinander stehen und entweder der eine (Art. 6) gilt, wenn es sich nicht um besondere Kategorien personenbezogener Daten handelt oder der andere (Art. 9), wenn es um besondere Kategorien personenbezogener Daten geht. Eine andere Auffassung ist, dass Art. 6 immer gilt und im Fall von besonderen Kategorien personenbezogener Daten darüber hinaus auch noch die Bedingungen von Art. 9, dass in diesem Fall also ein zweites Verbot mit Erlaubnisvorbehalt hinzukommt.

Ein formales Argument für diese zweite Sichtweise, der sich auch der Autor dieses Artikels anschließt, liegt im Wortlaut von Art. 6 Abs. 1 Satz 1 DSGVO:
„Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:" – danach kommt die vollständige Aufzählung der sechs Optionen a – f.

Dort steht nicht, dass es über die sechs Optionen hinaus weitere Fälle einer rechtmäßigen Verarbeitung geben kann. So gesehen muss es sich bei Art. 9 um zusätzliche Bedingungen handeln die zur allgemeinen Rechtmäßigkeit von Art. 6 im Fall von besonderen Kategorien personenbezogener Daten noch hinzukommen.

Ein anderer – inhaltlicher – Punkt für diese Interpretation der DSGVO ist im Art. 9 Abs. 2 lit e DSGVO zu finden. Dort steht als eine der Optionen, wann auch die Verarbeitung besonderer Kategorien personenbezogener Daten erlaubt ist: „die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat".

Das ist insofern interessant, als es diese Rechtsgrundlage bei Art. 6 Abs. 1 DSGVO (also für „normale" personenbezogene Daten) nicht gibt. Auch hierzu gibt es wieder zwei Auffassungen:

a Nach der einen Auffassung ist dies ein Beleg für die handwerklich schlecht gemachte DSGVO, denn es kann nicht gewollt sein, dass etwas nur für besondere Kategorien personenbezogener Daten erlaubt ist, für die normalen personenbezogenen Daten aber nicht. Angeblich steht das dort aber.

b Nach der anderen Auffassung lässt sich hier jedoch ableiten, dass der im Art. 9 Abs. 2 lit e DSGVO beschriebene Fall auch für normale personenbezogene Daten gilt. Als Rechtsgrundlage im Sinne des Art. 6 Abs. 1 DSGVO müsste man sich dann auf lit f (berechtigtes Interesse des Betroffenen) beziehen. Dagegen gibt es jedoch auch ein Widerspruchsrecht, das dann auch für besondere Kategorien personenbezogener Daten gilt. Im Art. 9 DSGVO steht zwar kein Widerspruchsrecht, aber das ist auch nicht nötig, wenn Art. 9 DSGVO nur ergänzend zu Art. 6 DSGVO zur Anwendung kommt und nicht alternativ dazu. So gesehen gibt es keinen Widerspruch und alles ergibt Sinn.

8. Beispiel: „Risikoabschätzung" – ein Henne-Ei-Problem

Art. 35 „Datenschutz-Folgenabschätzung" (DSFA) Abs. 1 Satz 1 DSGVO lautet:
„Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch."

Die „Risikoabschätzung" (die Bestimmung des Risikos einer Verarbeitung) findet also unabhängig von einer DSFA in jedem Fall statt. Vom Ergebnis des ermittelten Risikos hängt es dann ab, ob eine DSFA durchzuführen ist. Das Ergebnis einer DSFA ist demnach die Bestimmung der Folgen des Risikos für die betroffene Person – und nicht das Risiko selbst.

Art. 36 „Vorherige Konsultation" Abs. 1 DSGVO lautet:
„Der Verantwortliche konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung gemäß Artikel 35 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft."

Hier steht nun, dass das Risiko das Ergebnis einer DSFA ist. Das Risiko ist somit Voraussetzung und Ergebnis der DSFA. Gemeint ist vermutlich ein in der DSFA aktualisiertes/konkretisiertes Risiko, aber das steht dort nicht und das ist vermutlich eine der Ursachen für die vielen Fragen zu diesem Thema.

Eine weitere sprachliche Ungenauigkeit besteht bei diesem Abs. 1 in der Aussage, dass die Konsultation der Aufsichtsbehörde (nur) stattfinden muss, „sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft". Eigentlich ist die Aussage nicht ungenau, sondern sehr präzise – aber vermutlich anders gemeint. Denn bei wörtlicher Auslegung steht dort, dass eine einzige umgesetzte Maßnahme (unabhängig von der Höhe des Risikos und unabhängig davon, wie sehr das Risiko durch weitere ggf. leicht umzusetzende Maßnahmen erheblich reduzierbar wäre) reichen würde, um die Konsultation der Aufsichtsbehörde zu umgehen. Es ist schwer vorstellbar, dass dies die vom Gesetzgeber[27] intendierte Aussage sein sollte.

In der „Info 6"[28] der[29] Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) steht im Kap. 4.4 (S. 24) hierzu:
„Zeigt die Datenschutz-Folgenabschätzung ein verbleibendes hohes Risiko, muss zudem die Datenschutzaufsichtsbehörde konsultiert werden (Art. 36 Abs. 1 DSGVO)."

Nein – das steht so definitiv nicht dort (s. oben). Das Problem bei dieser Auslegung ist außerdem, dass hier die umgesetzten Maßnahmen keine Rolle spielen, was vermutlich so auch nicht gemeint war.

Konsequent ist daher auch, dass die (neuere) „Info 1"[30] der BfDI diesen Absatz ersatzlos gestrichen hat. Die neue Info-Broschüre enthält tatsächlich gar nichts zur DSFA. Das ist zwar nicht hilfreich aber auch nicht falsch.

9. Beispiel: Gibt es in der DSGVO (k)eine allgemeine Löschpflicht?

Vor etwa einem Jahr war vereinzelt die Meinung bzw. Behauptung zu hören, dass es in der DSGVO keine allgemeine Löschpflicht mehr gäbe, sondern nur noch auf Verlangen der betroffenen Person. Das schien zunächst schwer nachvollziehbar zu sein, denn es gibt ja den Art. 17 DSGVO, der eine Löschung unter den dort angegebenen Bedingungen klar fordert. Der Art. 17 Abs. 1 DSGVO lautet:

„Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

a Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

b Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

c Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.

d Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

e Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

f Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben."

Wenn man das liest, scheint spätestens ab dem Ende des Buchstaben „a)" klar zu sein, dass die personenbezogenen Daten zu löschen sind, wenn sie „nicht mehr notwendig" sind – und zwar unabhängig davon, ob der Betroffene das gefordert hat oder nicht.

Woher kommt dann diese andere Interpretation, die man beim besten Willen hier nicht herauslesen kann? Das Wort „notwendig" am Ende des Buchstaben „a)" verwundert zwar und man fragt sich, warum hier nicht wie ansonsten in der DSGVO (und im BDSG – alt wie neu) üblich, stattdessen „erforderlich" steht, aber das kann nicht solche Auswirkungen haben. Außerdem zeigt ein Vergleich mit der englischen Verhandlungssprache der DSGVO, dass dort „necessary" steht – also genau der Begriff, der ansonsten immer mit „erforderlich" übersetzt wird. Der Begriff „notwendig" hat also keinerlei Bedeutung, sondern ist mal wieder eine künstlerische Note der ~~Schweinez~~... Übersetzer, die sich offensichtlich gelangweilt hatten und etwas Abwechslung in den Text bringen wollten.

Handelt es sich bei der Aussage, dass es die Löschpflicht in der DSGVO nur noch sehr eingeschränkt gibt (wenn es der Betroffene verlangt und außerdem die übrigen Voraussetzungen dafür erfüllt sind) nur um eine vernachlässigbare Einzelmeinung? Bei der Recherche nach der Quelle für diese Aussage wurde der Autor auf die Kommentare „Schaffland/Wiltfang"[31] zum Art. 17 DSGVO verwiesen. Dort steht tatsächlich bei Rdn. 1 Abs. 2:

„Der wesentliche Unterschied zum BDSG 2003 liegt darin, dass der Verantwortliche nicht mehr per se zur Löschung verpflichtet ist, wie dies § 34 Abs. 2 Satz 2 BDSG 2003 vorsah, wenn einer der Tatbestände des Abs. 1 vorliegt, sondern nur, wenn der Betroffene dies verlangt, also einen entsprechenden Antrag stellt. Es liegt folglich an ihm, tätig zu werden, wenn seine Daten gelöscht werden sollen. Dieser Fall wird damit in der Praxis der Ausnahmefall bleiben und entlastet die Praxis. Gleichwohl bietet es sich an, Daten, die nicht mehr benötigt werden, zu löschen."

Es handelt sich also nicht um eine vernachlässigbare Einzelmeinung, sondern um eines der Standardwerke zum Datenschutz und somit um einen sehr verbreiteten Kommentar. Auch beim mehrfachen Nachlesen des Art. 17 Abs. 1 DSGVO kann der Autor die hier dargestellte Interpretation nicht nachvollziehen. Von einem Juristen einer auf Datenschutz spezialisierten Anwaltskanzlei erfuhr der Autor dieses Artikels dann, dass das „und" von „und der Verantwortliche ist verpflichtet" von den Kommentatoren vermutlich als UND-Verknüpfung interpretiert wurde, sodass immer beide Bedingungen (vor und hinter dem „und") erfüllt sein müssten. Der Jurist distanzierte sich jedoch sofort von dieser Interpretation, die er selbst nicht teilen würde.

Abgesehen davon, dass der Kommentar mit der angegebenen Referenz auf den § 34 BDSG-alt offensichtlich einen Tippfehler enthielt[32], ist die Interpretation der Kommentatoren trotz dieses Hinweises auf die UND-Verknüpfung nicht nachvollziehbar. Das Ganze erinnert an eine Szene aus einem Heinz Erhardt Film[33]:

> Heinz Erhardt steht als Beamter hinter einem geschlossenen Schalter. Ein Bürger, der ein Anliegen hat, klopft ans Fenster und Heinz Erhardt fragt: „Was wollen Sie? Sehen Sie nicht, dass geschlossen ist?" Der Bürger antwortet: „Auf dem Schild hier steht, dass Dienstag und Freitag geöffnet ist und heute ist Dienstag." Heinz Erhardt antwortet: „Ja – aber nicht Freitag."

Ein Komiker wie Heinz Erhardt darf so argumentieren und man kann sogar darüber lachen. Aber: Darf man das auch in einem juristischen Kommentar[34]?

Während der Autor über diese Frage nachdachte, ist ihm noch eine zweite (selbst erlebte) Geschichte eingefallen. Ein Teilnehmer meldete sich während einer der größten jährlich stattfindenden Datenschutzveranstaltungen in Deutschland zu Wort und begann seine Frage/Rede mit:

„Die Aufgabe von uns Juristen ist es ja oft, Rechtsunsicherheit herzustellen..."

Obwohl sicher die Hälfte der Teilnehmer Juristen waren, gab es nirgends einen Widerspruch. Man konnte nur sehen, dass viele grinsten, sich Blicke zuwarfen oder versteinert auf die Füße starrten.

10. Beispiel: Unsinnige Einwilligungen

Ein Thema, mit dem jeder Bürger und speziell jeder Datenschutzbeauftragte im letzten Jahr massiv konfrontiert war, ist die Flut an (meist unsinnigen) Einwilligungen, die einem zur Unterschrift vorgelegt werden. Dabei handelt es sich in diesem Fall nicht um eine problematische Formulierung im Gesetz, sondern nur um das, was fälschlicherweise aus dem Gesetz gemacht wurde.

In vielen Fällen war den Verantwortlichen dieser Formulare einfach nur der Unterschied zwischen Informationspflicht nach Art. 13 DSGVO und Einwilligung als Rechtsgrundlage nach Art. 6 Abs. 1 lit a DSGVO nicht klar. Anstatt die Informationspflicht z. B. mit einer Datenschutzerklärung umzusetzen, über die man informiert wird oder die man bestenfalls (z. B. per schriftlicher Bestätigung) zur Kenntnis nehmen kann, wurde oft bei der Unterschrift das „Einverständnis" verlangt. Damit handelt es sich dann aber nicht mehr um reine Information, sondern um eine Einwilligung. Das Problem dabei ist, dass eine Einwilligung immer freiwillig sein muss und auch jederzeit widerrufen werden kann.

Prozesse, bei denen man darauf angewiesen ist, dass sie mit allen Beteiligten gleichermaßen durchgeführt werden, können daher nicht auf einer Einwilligung beruhen. Das ist aber auch gar nicht nötig, denn wenn man auf eine Einwilligung nicht verzichten bzw. einen Widerruf nicht umsetzen kann, dann ist die Verarbeitung der Daten offensichtlich (z. B. aufgrund eines Gesetzes oder zur Erfüllung eines Vertrages mit dem Betroffenen) erforderlich und dafür gibt es eigene Rechtsgrundlagen (z. B. Art. 6 Abs. 1 lit b oder lit c DSGVO). Eine Einwilligung braucht man dann nicht mehr. Wenn man aber nach dem Motto „sicher ist sicher" trotzdem zusätzlich eine Einwilligung einholt, dann geht man nicht auf Nummer sicher, sondern man schafft sich so erst das oben genannte Problem mit dem Widerspruchsrecht (bzw. dem Risiko, dass die Einwilligung von Anfang an nicht gegeben wird).

Hier handelt es sich im Ergebnis sicher um das größte globale Kundenvernichtungsprogramm der letzten Jahrzehnte. Sehr viele Unternehmen haben aufgrund der DSGVO (bzw. der neuen Bußgelder der DSGVO) alle Kunden mit entsprechenden Einwilligungsformularen angeschrieben. Das ist umso erstaunlicher, als sich die Rechtslage durch die DSGVO gegenüber dem alten BDSG in der Sache gar nicht geändert hat. Wer also bisher keine Einwilligung brauchte, braucht sie auch jetzt nicht, weil die alte Rechtsgrundlage nach wie vor gilt. Wer bisher keine Rechtsgrundlage hatte, brauchte zwar eine, aber das hat dann nichts mit der DSGVO zu tun, denn die Rechtsgrundlage wäre ja auch vor dem 25. Mai 2018 bereits erforderlich gewesen. Ärgerlich ist in diesem Zusammenhang, dass dieses Chaos der DSGVO zugeschrieben wird.

Die betroffenen Personen waren im Normalfall spätestens nach der 3. oder 4. Einwilligung dieser Kategorie genervt und haben sie nur noch weggeworfen. Damit konnten diese „Kunden" dann aber auch aus den Unternehmensdatenbanken entfernt werden, denn selbst wenn man bisher eine Rechtsgrundlage zur Verarbeitung von deren Daten hatte, hatte man sie nun ggf. (mindestens für den im Einwilligungsformular angegebenen Zweck) nicht mehr. Nach allgemeiner Rechtsauffassung kann man in so einem Fall nicht ersatzweise wieder auf eine andere Rechtsgrundlage zurückgreifen. Wenn man das könnte, würde die Freiwilligkeit der Einwilligungen und deren Widerspruchsrecht keinen Sinn mehr machen.

Es scheint klar zu sein, dass die verbreitete Unsitte mit den überflüssigen Einwilligungen nicht von Datenschutzexperten in die Welt gesetzt worden sein kann[35]. Es muss also Kreise außerhalb der Datenschutzbeauftragten geben, die sich im Datenschutzrecht zwar nicht auskennen, aber trotzdem diesbezüglich beraten[36] und entsprechende Einwilligungsformulare entwerfen.

Wenn man sich vor diesem Hintergrund einmal ausmalt, was passiert wäre, wenn die Gesetzesinitiative von Bayern und Baden-Württemberg (siehe Beispiel 6 Abs. 1) durchgegangen wäre…

Nachtrag – kurz vor Redaktionsschluss: Zu dem in den anderen Artikeln dieses Heftes angesprochenen Entschließungsantrag des Landes Niedersachsen zu diesem Thema sagt der aktuelle BfDI (Ulrich Kelber), dass ein Wegfall der Datenschutzbeauftragten keinen Bürokratie- sondern einen Kompetenzabbau zur Folge hätte. Dem kann man nur uneingeschränkt zustimmen.

Fazit

Es wird noch lange nicht langweilig.

1 Das komplette Heft ist unter https://www.datenschutzverein.de/wp-content/uploads/2018/08/DANA_17_3_Sonderheft-40_Jahre_DVD.pdf abrufbar.

2 Im folgenden Text ist mit „BDSG" immer das neue BDSG (ab 25. Mai 2018) gemeint, sofern es nicht ausdrücklich anders angegeben ist.

3 Mit Ausnahme einer Fußnote auf Seite 107, zum Erwägungsgrund 173 DSGVO bezüglich der „Datenschutzrichtlinie für elektronische Kommunikation": „Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37)"

4 Das ist auch die deutsche Übersetzung im oben erwähnten Erwägungsgrund 173 der DSGVO (s. auch Endnote 3).

6 Hier handelt es sich um eine Ergänzung zum Beispiel 2 des Artikels über die Kuriositäten in der DANA 3/2017. Zu selbstbezüglichen Sätzen und den daraus resultierenden Problemen siehe auch die Beispiele 6 und 9 des Artikels von damals.

7 Im alten BDSG gab es diese Einschränkung auch – in den §§ 12 und 27.

8 Siehe: https://de.wikipedia.org/wiki/Unbestimmter_Ausdruck_(Mathematik)

9 Siehe: https://de.wikipedia.org/wiki/Eulersche_Zahl

10 $(1+\frac{1}{n})$ ist gleich 1, wenn „n" unendlich groß wird.

11 Das ist bei $1+\frac{1}{n}$ für noch so große Werte von n immer der Fall.

12 Der Autor outet sich hiermit als Heinz Erhardt Fan (noch'n Gedicht), wie insbesondere am Beispiel 9 unschwer zu erkennen ist.

13 www.eurocontrol.int/

14 Siehe hierzu auch wieder Beispiel 2 des Artikels über die Kuriositäten in der DANA 3/2017

15 Im alten BDSG wurde „nicht-öffentlich“ noch mit Bindestrich geschrieben.

16 Beispielsweise steht im Art. 35 (Datenschutz-Folgenabschätzung - DSFA) Abs. 3 lit c DSGVO, dass eine DSFA erforderlich ist, wenn eine „systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche“ vorliegt.

17 Siehe Art. 21 Abs. 1 DSGVO

18 Siehe Art. 13 Abs. 2 lit b DSGVO

19 Siehe Art. 13 Abs. 1 lit d DSGVO

20 Siehe zum Begriff „fair“ das Beispiel 4 des Artikels über die Kuriositäten in der DANA 3/2017

21 Siehe z.B. https://www.datenschutzverein.de/wp-content/uploads/2016/11/Stellungnahme_Videoueberwachung_06112016.pdf

22 Siehe: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:C:2016:202:FULL&from=DE

23 Siehe: www.bundestag.de/blob/409512/4afc3a566097171a7902374da77cc7ad/a-drs-18-24-94-data.pdf

24 Dort steht, dass Verantwortliche einen DSB auch dann zu benennen haben, „soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen“.

25 Siehe hierzu auch ausführlich das Beispiel 4.

27 Die Interpretation der am Gesetzgebungsprozess beteiligten Lobbyisten war eventuell genau die hier dargestellte.

28 Siehe: www.uni-paderborn.de/fileadmin/datenschutz/INF06.pdf

29 Als die Info 6 entstand und auch als die später im Text erwähnte Info 1 überarbeitet wurde, war noch Frau Voßhoff die BfDI, und noch nicht Herr Kelber, so dass es hier im Text bewusst „die BfDI“ bzw. „der Bundesbeauftragten“ heißt.

30 Siehe: www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO1.pdf

31 DSGVO Datenschutz-Grundverordnung Kommentar Schaffland/Wiltfang, Erich Schmidt Verlag, ISBN 978 3 503 17404 1

32 Die Löschung bei nicht-öffentlichen Stellen war Thema des § 35 BDSG-alt.

33 Die Geschichte ist nur sinngemäß wiedergegeben. An den genauen Wortlaut oder den Titel des Films erinnert sich der Autor nicht mehr.

34 Dieser Satz ist ausdrücklich nicht als selbstbezüglicher Satz zu verstehen – diese Aussage bezieht sich auf den Satz im Text mit der Endnote am Ende und nicht auf diesen Satz in der Endnote.

35 Der Autor ist in mehreren Datenschutzvereinen Mitglied und ist überall auf dieselben Erfahrungen mit diesen unsinnigen Einwilligungen gestoßen. Niemand dort hatte dazu eine andere Meinung.

36 Gemeint sind Kreise, die befugt sind, Rechtsauskünfte – auch im DS-Recht – zu geben, obwohl sie keine Datenschutzbeauftragten sind. Diejenigen, die sich intensiv mit dem DS-Recht befasst haben, obwohl sie keine Datenschutzbeauftragten sind, sind hier ausdrücklich nicht gemeint.

Andrea Backer-Heuvedop

Quo vadis, Datenschutzbeauftragter?

Der betriebliche Datenschutzbeauftragte stellt in Deutschland ein seit über 40 Jahren bewährtes Instrument zum Schutz personenbezogener Daten dar, das bereits im „Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung“ vom 27. Januar 1977 Voraussetzungen enthielt. Dabei handelte es sich in § 28 BDSG 1977[1] um strengere Voraussetzungen für eine solche Bestellung als es zum Zeitpunkt der Anwendbarkeit der EU-Datenschutzgrundverordnung (EU-DSGVO) der Fall war. Mit der EU-Datenschutzgrundverordnung (EU-DSGVO) dehnt der Datenschutzbeauftragte seinen Wirkungsgrad nun auf alle Mitgliedsstaaten aus. Der EU-Gesetzgeber hat den Mitgliedsstaaten jedoch Spielräume durch Art. 37 Abs. 4 S. 1 Hs. 2 EU-DSGVO eröffnet, der es ihnen ermöglicht, von den Voraussetzungen der EU-DSGVO für die Benennung abzuweichen. So werden in § 38 Abs. 1 BDSG in Deutschland zusätzliche Fälle geregelt, in denen nichtöffentliche Verantwortliche einen Datenschutzbeauftragten benennen müssen, die eine große inhaltliche Kontinuität zur letzten Fassung des BDSG in § 4f BDSG alte Fassung aufweist.

Demnach müssen Verantwortliche und Auftragsverarbeiter im Anwendungsbereich des BDSG unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen einen Datenschutzbeauftragten benennen, wenn

a in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden oder
b Verarbeitungen vorgenommen werden, die einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO unterliegen oder
c personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden.

Während die Rufe nach standardisierter Qualifikation des Datenschutzbeauftragten zu Recht zunehmend lauter werden, da weder die EU-DSGVO noch das BDSG spezifische Anforderungen hinsichtlich seiner Fachkenntnisse oder Ausbildung vorsehen, werden in den Mitgliedsstaaten neue Berufsverbände für Datenschutzbeauftragte gegründet.

Zeitgleich wird hingegen in Deutschland immer wieder die Benennungspflicht des Datenschutzbeauftragten zum Gegenstand genommen, um vermeintliche Entlastungen für den Mittelstand und für Vereine zu diskutieren, wie zuletzt zum Beispiel durch den Entschließungsantrag des Landes Niedersachsen an den Bundesrat zur Änderung

datenschutzrechtlicher Bestimmungen vom 02.04.2019[2].

Mit Anwendbarkeit der EU-DSGVO kam es auch zu einer Änderung des Aufgabenkatalogs des Datenschutzbeauftragen. Bezüglich der neueren Anteile dieses Aufgabenkatalogs wurden im ersten Jahr der Anwendbarkeit der EU-DSGVO die ersten Gehversuche gemacht, sie bedürfen aber bezüglich ihrer Ausfüllung noch einer Weiterentwicklung in Richtung abgestimmter Best Practices anhand der Umsetzungserfahrungen dieses ersten Jahres.

Dieser Artikel soll Hinweise zur Beantwortung der Fragestellungen geben, welche Kriterien Verantwortliche und Auftragsverarbeiter bei der Entscheidung des für sie richtigen Datenschutzbeauftragten derzeit anlegen können, ob ein Wegfall oder eine Senkung der Benennungspflicht tatsächlich die beabsichtigten Entlastungseffekte schaffen kann und welche Erfahrungen bezüglich der neu geregelten Teile der gesetzlichen Aufgaben des Datenschutzbeauftragten festzustellen sind.

Anforderungen an die Qualifikation des Datenschutzbeauftragten

Gemäß der Rechtsprechung des Bundesfinanzhofs (BFH) vor Anwendbarkeit der EU-DSGVO handelt es sich beim Datenschutzbeauftragten um ein eigenständiges Berufsbild, das lt. BFH auf Grund des bezeichneten Anforderungsprofils nur dann mit der erforderlichen Fachkunde ausgeübt werden kann, wenn der Funktionsträger theoretisches Grundwissen aus diversen Lehrinhalten von Hoch- bzw. Fachhochschulstudiengängen (Ingenieur-, Rechtswissenschaften, Betriebswirtschaftslehre und Pädagogik) aufweisen kann. Dabei erstrecke sich der erforderliche interdisziplinäre Wissensstand aber nur auf Teilbereiche dieser Studiengänge, so dass es weder der Absolvierung, noch des Abschlusses eines dieser Hoch- bzw. Fachhochschulstudiengänge bedürfe. Der Datenschutzbeauftragte leistet demzufolge eine Beratungsleistung auf interdisziplinären Wissensgebieten.

Die Auffassung, dass sich aufgrund der Komplexität der datenschutzrechtlichen Regelungen in EU-DSGVO, BDSG und weiteren Vorschriften eine Erforderlichkeit dafür ergäbe, dass der Datenschutzbeauftragte ein Rechtsanwalt oder Volljurist sein sollte, wird den anderen Fachdisziplinen außerhalb der Rechtswissenschaften damit nicht gerecht. Ergänzend sei an dieser Stelle auch darauf hingewiesen, dass zunehmend spezialisierte Studiengänge mit interdisziplinären Ansätzen insbesondere an Fachhochschulen entwickelt wurden, die weite Teilbereiche des geforderten Fachwissens des Datenschutzbeauftragten beinhalten wie zum Beispiel Masterstudiengänge in Informationsrecht, Compliance & Datenschutz, Wirtschaftsrecht etc.

Aufgrund dieser Interdisziplinarität ist insbesondere die Überprüfung der Qualifikation einer Person, die die Funktion des Datenschutzbeauftragten übernehmen soll, für die Verantwortlichen und Auftragsverarbeiter nicht einfach, da der Nachweis eines bestimmten Studienganges allein offensichtlich gerade nicht ausreichen kann.

Aus Sicht der europäischen Aufsichtsbehörden in ihren Leitlinien[3] in Bezug auf Datenschutzbeauftragte ist die Entscheidung für die Benennung einer Person zum Datenschutzbeauftragten basierend auf deren beruflicher Qualifikation und insbesondere ihres Fachwissens zu treffen, das sie auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage der Fähigkeit zur Erfüllung ihrer Aufgaben[4]

Wie also können Verantwortliche und Auftragsverarbeiter unter diesen Rahmenbedingungen ihren Entscheidungsprozess vereinfachen und überprüfbar gestalten?

Leider noch zu wenig bekannt scheint, dass der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. bereits seit 2009 Anforderungen an die Tätigkeit und das Know-how des Datenschutzbeauftragten in seiner Publikation „Das berufliche Leitbild der Datenschutzbeauftragten"[5] definiert, die inzwischen bereits als 4. Ausgabe 2018 vorliegt.

Voraussetzungen der Berufsausübung als Datenschutzbeauftragte sind nach diesem Leitbild, dass der Funktionsträger

- mindestens eine angemessene berufliche Qualifikation in zumindest einer der Kategorien Organisation und Prozesse, Informations- und Kommunikationstechnologie (IuK) oder Recht besitzt und solides Fachwissen in den beiden anderen Kategorien erworben hat,
- über eine mindestens 2-jährige Berufserfahrung in den genannten Bereichen verfügt und
- eine anerkannte Qualifikation zum Datenschutzbeauftragten erlangt hat.

Zudem wird das erforderliche Fachwissen in den Bereichen Datenschutzrecht, Informations- und Kommunikationstechnologie, Betriebswirtschaft und Organisation vorausgesetzt und um bestimmte persönliche Voraussetzungen ergänzt. Mit Abgabe der schriftlichen „Selbstverpflichtung auf das berufliche Leitbild des Datenschutzbeauftragten" und bei entsprechendem Fachkundeerhaltungsnachweis können derart qualifizierte Mitglieder durch den BvD bereits heute als entsprechend qualifiziert ausgezeichnet werden. Der BvD führt ein Verzeichnis der externen Datenschutzbeauftragten[6], die sich auf das berufliche Leitbild des Datenschutzbeauftragen verpflichtet haben.

Kann der Wegfall der Benennungspflicht kleine und mittlere Unternehmen und Vereine entlasten?

Kernpunkt der Kritik an den in Deutschland geltenden Benennungsvoraussetzungen sind daraus vermeintlich resultierende finanzielle und bürokratische Benachteiligungen von insbesondere kleinen und mittleren in Deutschland ansässigen Unternehmen (KMU) gegenüber Unternehmen in anderen Mitgliedsstaaten. Diese Mehrbelastung durch Bürokratie soll für KMU und Vereine durch die geltende Mindestanzahl von zehn Personen insbesondere durch Kosten für die Benennung eines Datenschutzbeauftragten sowie ggfs. dessen Aus- und Fortbildung bestehen.

Eine Entbindung von der Benennungspflicht entbindet jedoch in keiner Form von den datenschutzrechtlichen Pflichten der Unternehmen, Institutionen und Vereinen im Hinblick auf die Erfüllung der gesetzlichen Anforderungen. Die Pflicht zur Implementierung der erforderlichen internen Datenschutzorganisation bleibt bestehen.

Ein Wegfall der Benennungspflicht geht gerade nicht einher mit einem Wegfall der Pflicht, Datenschutzprozesse zur Erfüllung der Betroffenenrechte zu schaffen, technische und organisatori-

sche Maßnahmen zum Schutz der personenbezogenen Daten festzulegen und die datenschutzrechtlichen Dokumentationspflichten zu erfüllen.

Unberücksichtigt bleibt dabei, dass mit einem Wegfall der Benennungspflicht die Zielgruppe der kleinen und mittleren Unternehmen und Vereine lediglich die interne Beratungs- und Überwachungsinstanz für diese Vorgänge verliert. Dies geschieht zum Nachteil der betroffenen Personen, deren Daten verarbeitet werden, aber auch gegebenenfalls zum Nachteil der Zielgruppe selbst, wenn Versäumnisse in Unkenntnis begangen werden, auf die ein qualifizierter Datenschutzbeauftragter rechtzeitig hingewiesen hätte. So können Versäumnisse entstehen, deren Folgen nicht nur das Risiko von Bußgeldern, sondern auch das Risiko von Schadenersatzanforderungen oder Unterlassungsansprüchen beinhalten können. Anzunehmen, dass bei einem Wegfall oder einer Minderung der Benennungspflicht der für den Datenschutzbeauftragten „gesparte“ Aufwand als Budget zur Umsetzung des Datenschutzes im Unternehmen eingesetzt würde, erscheint wenig wahrscheinlich und selbst wenn dies im Einzelfall Intention sein sollte, müsste das Niveau des Fachwissens eines qualifizierten Datenschutzbeauftragten erst an anderer Stelle im Unternehmen aufgebaut werden.

Sowohl EU-DSGVO als auch BDSG beinhalten einen risikobasierten Ansatz, der das Risiko aus Sicht der betroffenen Personen im Fokus hält. Der Ruf nach einem Wegfall oder einer Minderung der Benennungspflicht allein mit der Begründung des Bürokratieabbaus und zur Generierung von Kosteneinsparungen für die Verantwortlichen und Auftragsverarbeiter und ohne dass diesem risikobasierten Ansatz konkret Rechnung getragen wird, wird der Verantwortung des Gesetzgebers nicht gerecht. Weder gegenüber der zu entlastenden Zielgruppe noch gegenüber den betroffenen Personen, deren Daten verarbeitet werden.

Wie entwickelt sich die Funktion des Datenschutzbeauftragten in Zukunft weiter?

Die Wahrnehmung der Funktion des Datenschutzbeauftragten ist seit Anwendbarkeit der EU-DSGVO nicht einfacher geworden. Eine Befragung der EU-Kommission[7] hat ergeben, dass europaweit inzwischen 67 % der Europäer und in Deutschland sogar 79 % von der EU-DSGVO gehört haben, 57 % (Deutschland 58 %) wissen, dass es eine Aufsichtsbehörde in ihrem Mitgliedsstaat für den Schutz ihrer personenbezogenen Daten gibt[8]. Die Aufsichtsbehörden in Deutschland verzeichnen eine steigende Anzahl an Anfragen und Beschwerden[9]. Das Bewusstsein für den Datenschutz ist für jedermann spürbar gestiegen, nicht nur bei den betroffenen Personen, sondern auch bei den Verantwortlichen und Auftragsverarbeitern. Mit diesem gestiegenen Bewusstsein erfolgte aber auch ein Erkenntnisgewinn in den Unternehmen und Vereinen über bestehende Unsicherheiten oder gar Defizite in der Erfüllung der Anforderungen des Datenschutzes bei der Verarbeitung personenbezogener Daten. Datenschutzbeauftragte erleben eine gestiegene Nachfrage nach Beratung in den vielfältigsten Themenbereichen und müssen nicht selten anhand ihres eigenen risikobasierten Maßstabs ihre Tätigkeit priorisieren.

Bei seiner Tätigkeit muss der Datenchutzbeauftragte gem. Art. 39 Abs. 2 EU-DSGVO „dem mit den Verarbeitungsvorgängen verbundenen Risiko“ unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung gebührend Rechnung tragen. Dies bedeutet aus Sicht der Aufsichtsbehörden in erster Linie eine Konzentration auf die Bereiche, von denen ein höheres Risiko ausgeht. Seine Aufgaben lassen sich in vier Kernsegmente unterteilen: die Unterrichtung und Beratung bei der Einhaltung der datenschutzrechtlichen Vorschriften, die Überwachung der Einhaltung der EU-DSGVO, seine Funktion im Rahmen einer vom Verantwortlichen durchzuführenden Datenschutz-Folgenabschätzung sowie seine Funktion als Anlaufstelle der Aufsichtsbehörde und seine Zusammenarbeit mit der Aufsichtsbehörde. Beratungs- und Überwachungsaufgaben sind dem Datenschutzbeauftragtem in Deutschland nicht fremd. In der Praxis noch weniger erprobt scheint jedoch noch seine Funktion als Ansprechpartner der Aufsichtsbehörden zu sein. Hier wird er in erster Linie eine Vermittlungsfunktion in der Kommunikation zwischen Verantwortlichem und Aufsichtsbehörde wahrnehmen, sobald die Aufsichtsbehörden ihn bei der Ausübung ihrer Untersuchungs-, Abhilfe-, Genehmigungs- und beratenden Befugnisse direkt adressieren.

Mit der ständig steigenden Digitalisierung in den Unternehmen wird auch die Bedeutung des Datenschutzbeauftragten zunehmen. Die Anforderungen an Fachwissen und Expertise werden mit dem Schutzbedarf der vom Verantwortlichen verarbeiteten personenbezogenen Daten steigen. Umso wünschenswerter ist eine verbindliche Konkretisierung der berufsrechtlichen Voraussetzungen an die Qualifikation des Datenschutzbeauftragten.

1 § 28 Bundesdatenschutzgesetz (1977), https://www.datenschutz-wiki.de/BDSG_1977

2 Entschließungsantrag des Landes Niedersachsen an den Bundesrat zur Änderung datenschutzrechtlicher Bestimmungen vom 02.04.2019, https://www.bundesrat.de/drs.html?id=206-19, siehe dazu auch https://www.datenschutzverein.de/wp-content/uploads/2019/04/2019-04-12-BR-Vorstoss-NDS-DSGVO.pdf

3 Leitlinien des EDPB in Bezug auf Datenschutzbeauftragte, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

4 auf seiner ersten Plenarsitzung gebilligte Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“) der Art. 29 Datenschutzgruppe; WP 243 rev.01; Seite 27

5 Das berufliche Leitbild der Datenschutzbeauftragten, https://www.bvdnet.de/wp-content/uploads/2018/04/BvD-Berufsbild_Auflage-4_dt_en.pdf

6 Verzeichnis der nach Verbandskriterien verpflichteten externen Datenschutzbeauftragten, Stand Oktober 2018, https://www.bvdnet.de/wp-content/uploads/2018/11/BvD_eDatenschutzbeauftragte_102018.pdf

7 Fragebogen der EU-Kommission Special Eurobarometer 487a – Wave EB91.2 – Kantar; Stand März 2019, http://ec.europa.eu/commfrontoffice/publicopinion//includes/images/mimetype/pdf1.gif

8 http://ec.europa.eu/commfrontoffice/publicopinion//includes/images/mimetype/pdf1.gif

9 https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/17_EinJahrDSGVO.html

Frank Spaeing

Ein Jahr DSGVO – ein Überblick über viele Rückblicke

Vorneweg, dies ist eine subjektive Zusammenstellung von verschiedensten Quellen. Zum einen habe ich die Suchmaschine meiner Wahl gestartet (https://www.startpage.com/de/) und in dieser als Suchbegriffe „ein jahr dsgvo" eingegeben (und dann sehr viel gelesen und subjektiv entschieden, was ich als Rückblick als sinnvoll und nicht zu sehr als Werbe- oder Interessengetrieben betrachtet habe), zum anderen habe ich andere Seiten und Dokumente, die mir vorher schon bekannt waren, mit in die Ergebnisliste aufgenommen. Und wie stelle ich das jetzt alles übersicht dar? Ich habe mich dafür entschieden, aus jeder Quelle einen Satz zu zitieren, der mich im jeweiligen Beitrag angesprochen hat. Und manchmal konnte ich mir einen Kommentar nicht verkneifen.

- „Die DSGVO im Spannungsverhältnis zwischen Umsetzung, Menschen mit verdichtetem Rechtsbewusstsein und der normativen Kraft des Faktischen" – https://media.ccc.de/v/glt19-36-ein-jahr-dsgvo-und-jetzt-/related – Wenn das mal nicht ein toller Titel ist. (Video 50 Minuten)
- „Lästig, aber notwendig: an den Datenschutz denken!" – https://www.facebook.com/Bundesregierung/videos/675439856218513/ – Und warum muss das auf Facebook sein, liebe Bundesregierung? (Video 1,5 Minuten)
- Vortrag von Katharina Nocun und Lars Hohl auf der re:publica 2019 – Best of DSGVO-Armageddon – https://www.youtube.com/watch?v=Q1EQU_HsNic (Video 58 Minuten)
- „SCHWERPUNKT: Ulrich Kelber, Bundesbeauftragter für Datenschutz und Informationsfreiheit, bilanziert ein Jahr DSGVO" – https://www.tagesschau.de/wirtschaft/ein-jahr-dsgvo-101.html (Video 6,5 Minuten)
- „Ein Jahr DSGVO – Stephan Hansen-Oest" – https://larsbobach.de/ein-jahr-dsgvo-stephan-hansen-oest/ – Der Datenschutz-Guru polarisiert gerne, hat aber auch oft Recht. (Audio 37 Minuten)
- „Bußgelder nach einem Jahr DSGVO" – https://www.juraforum.de/ratgeber/datenschutzrecht/ein-jahr-dsgvo
- „Ständig aktualisierte Seite zu Bußgeldern in der EU": http://www.enforcementtracker.com/
- „Dennoch zeigen erste Bußgelder, welche Datenschutzverstöße dringend vermieden werden sollten." – https://www.haerting.de/neuigkeit/ein-jahr-dsgvo
- „Es war teilweise überraschend, zu sehen, dass viele kleinere Unternehmen sich vor der DSGVO nur unzureichend mit dem Thema Datenschutz auseinandergesetzt hatten und die Anforderungen des alten Bundesdatenschutzgesetzes häufig nicht erfüllten." – https://www.wbs-law.de/datenschutzrecht/ein-jahr-dsgvo-eine-bilanz-aus-der-anwaltspraxis-80330/
- „Auch ein Jahr nach ihrem Inkrafttreten führt die DSGVO damit weiterhin zu intensiven politischen Diskussionen." – https://www.golem.de/news/ein-jahr-dsgvo-datenschutzbeschwerden-bleiben-auf-hohem-niveau-1905-141477.html
- „Ein Drittel der Manager in deutschen Unternehmen gibt zu, vom Thema DSGVO zwar gehört zu haben, aber nicht zu wissen, worum es dabei konkret geht." – https://blog.wiwo.de/look-at-it/2019/05/27/ein-jahr-dsgvo-nutzung-von-whatsapp-auf-job-smartphones-im-vergleich-zu-2018-gestiegen/
- „Vor einigen Jahren hätte sich wohl kaum ein Apotheker träumen lassen, in welchem Umfang er sich einmal mit dem Datenschutz befassen würde." – https://www.deutsche-apotheker-zeitung.de/news/artikel/2019/05/27/ein-jahr-dsgvo-verstaerkte-kontrollen-geplant – Hatten sie sich denn vorher nicht mit dem Datenschutz beschäftigt?
- „Wernicke für Überarbeitung der Datenschutzregeln" – https://www.dihk.de/presse/meldungen/2019-05-23-dsgvo-umfrage – Wer hätte diese Meinung erwartet?
- „DSGVO, bekannt aber nicht vollständig verstanden." – https://de.statista.com/infografik/18136/daten-zu-bekanntheit-und-anwendung-der-dsgvo/ – Bilder sagen mehr als Worte.
- „Die Datenschutz-Grundverordnung hat die Landschaft in Europa und darüber hinaus verändert." – http://europa.eu/rapid/press-release_IP-19-2610_de.htm – Auch die EU zieht eine Bilanz.
- „Ein Jahr DSGVO - Zwölf Monate, zwölf Meinungen" – https://netzpolitik.org/2019/ein-jahr-datenschutzgrundverordnung-zwoelf-monate-zwoelf-meinungen/ – Lesenswert!
- „Die DSGVO ist ein Gewinn für Verbraucher." – https://www.vzbv.de/pressemitteilung/ein-jahr-dsgvo-besserer-datenschutz-fuer-verbraucher
- „Handlungsdruck nimmt zu" – https://www.security-insider.de/ein-jahr-dsgvo-viel-laerm-um-nichts-a-832854/
- „Die meisten können eigentlich ganz gut leben mit der DSGVO." – https://www.deutschlandfunknova.de/beitrag/datenschutzgrundverordnung-ein-jahr-dsgvo
- „Verwirrung und Unsicherheit – ein Jahr DSGVO" – https://www.handelsblatt.com/politik/deutschland/datenschutz-verwirrung-und-unsicherheit-ein-jahr-dsgvo/24361014.html
- „DSGVO-Hysterie – Ein Jahr nach dem Weltuntergang" – https://www.spiegel.de/netzwelt/netzpolitik/dsgvo-mythen-aus-dem-ersten-jahr-datenschutz-grundverordnung-a-1265926.html
- „Ein Jahr Schreckgespenst DSGVO" – https://www.it-business.de/ein-jahr-schreckgespenst-dsgvo-a-830523/
- „Ein Jahr DSGVO: Höhere Datenhygiene und mehr Bürokratie" – https://www.digitalbusiness-cloud.de/ein-jahr-dsgvo-hoehere-datenhygiene-und-mehr-buerokratie – Datenhygiene, das ist doch mal ein schönes Wort…
- „1 Jahr DSGVO: So skurril und weltfremd läuft es in der Praxis wirklich ab" – https://neuhandeln.de/1-jahr-dsgvo-so-skurill-und-weltfremd-laeuft-es-in-der-praxis-wirklich-ab/ – Ich bin mir

nicht sicher, was der Autor uns genau sagen will…

- „Kultureinrichtungen haben kaum Probleme mit DSGVO" – https://www.mdr.de/kultur/datenschutz-grundverordnung-kultur-100.html – Echt?
- „Kommentar: Ein Jahr DSGVO - ein Grund zum Feiern!" – https://heise.de/-4433915 – Peter Schaar bilanziert Erfolg
- „Datenschutz im digitalen Zeitalter: Umsetzung der Datenschutzgrundverordnung (DSGVO) – Bilanz ein Jahr nach Inkrafttreten Gutachten im Auftrag der Fraktion Bündnis 90/Die Grünen im Deutschen Bundestag – Peter Schaar, Dr. Alexander Dix" – https://www.gruene-bundestag.de/fileadmin/media/gruenebundestag_de/themen_az/datenschutz/Gutachten_DSGVO.pdf
- „Ein Jahr DSGVO: Erfolge und Schwierigkeiten des neuen Datenschutzrechts" – https://heise.de/-4431402 – Eine lesenswerte Sammlung.

Und das ist er, der subjektive Überblick über viele Rückblicke. Vielleicht finden Sie ja die eine oder andere Quelle interessant genug, um weiterzulesen.

DVD-Presserklärung vom 12.04.2019

Niedersachsen: Datenschutzfreie Regierung?

Die Deutsche Vereinigung für Datenschutz e. V. (DVD) hat mit größtem Befremden einen Bundesrats-Antrag der Niedersächsischen Landesregierung zur Kenntnis genommen, in dem diese fordert, im Interesse der „Entlastung von kleinen und mittleren Unternehmen von zusätzlichen Bürokratiekosten" die Pflicht zur Benennung von Datenschutzbeauftragten aufzuweichen und eingetragene Vereine mit überwiegend ehrenamtlich Tätigen von dieser Pflicht möglicherweise völlig auszunehmen. Außerdem sollen die Fristen zur Benachrichtigung von Datenschutzverletzungen verlängert, die Abmahnmöglichkeit von Datenschutzverstößen ausgeschlossen sowie die Nutzung von Echtdaten für „Erprobungs- und Testzwecke" generell erlaubt werden (BR-Drucksache. 144/19 vom 03.04.2019).

Angesichts dieses Antrags stellt sich die DVD die Frage, ob die niedersächsische Landesregierung bereits im Informationszeitalter angekommen ist: Seit dem Wirksamwerden der europaweit geltenden Datenschutz-Grundverordnung (DSGVO) im Mai 2018 startet sie einen Angriff auf den Datenschutz nach dem nächsten: So erließ sie ein Landesdatenschutzrecht, das die hochsensible Datenverarbeitung durch Strafverfolger von der Datenschutzkontrolle „befreit", was unzweifelhaft gegen deutsches Verfassungsrecht sowie gegen Europarecht verstößt.

Mit der aktuellen Initiative will die Landesregierung das Datenschutzrecht ins vorherige Jahrhundert zurückversetzen. Tatsächlich gilt der derzeit gültige Vorrang der Selbstkontrolle beim Datenschutz in Deutschland schon seit Jahrzehnten und hat sich bewährt. Es gibt wohl keine mittelständischen Unternehmen und keine Vereine, die heute nicht im Internet präsent sind und mindestens deshalb Grundwissen über den Datenschutz vorhalten müssen. Wenn dort keine Datenschutzbeauftragten beratend und überwachend tätig werden, gibt es erfahrungsgemäß nur selten die notwendige Kompetenz.

Frank Spaeing, Vorsitzender der DVD: „Die Pflicht abzuschaffen, Datenschutzbeauftragte zu benennen, entlastet die KMU und Vereine nur scheinbar. Denn keine der diversen Pflichten, die die DSGVO (zurecht) Verantwortlichen auferlegt, wird dadurch wegrationalisiert. Einzig die Fachkompetenz, die durch Datenschutzbeauftragte üblicherweise bei Verantwortlichen Einzug hält, verschwindet. Zudem gab es die meisten Pflichten, die durch die DSGVO jetzt so viel Prominenz erfahren haben, schon seit vielen Jahren. Nur wurden sie geflissentlich durch die Verantwortlichen ignoriert und auch durch die drastisch unterbesetzten Aufsichtsbehörden regelmäßig nicht im nötigen Umfang geahndet. Die Landesregierung schreibt im Entwurf zurecht, dass zu viel Rechtsunsicherheit besteht. Den Verantwortlichen nun auch noch die Kompetenz, die sie durch Datenschutzbeauftragte bekommen können, wegzunehmen, ist aber der falsche Weg. Besser wäre es, die Aufsichtsbehörden so auszustatten, dass sie wirksam in der Breite unterstützen können."

Riko Pieper, stellvertretender Vorstandsvorsitzender der DVD: „Die Benennung eines Datenschutzbeauftragten ist nicht Bürokratie, sondern Selbstschutz. Diese Aufgabe kann von einem Mitarbeiter oder einem Ehrenamtlichen wahrgenommen werden; die nötigen Kompetenzen können im Rahmen von ohnehin nötigen Fortbildungen erworben werden. Ohne sie begibt sich ein Vorstand oder eine Unternehmensleitung in ein unkalkulierbares Existenzrisiko."

Werner Hülsmann, stellvertretender Vorstandsvorsitzender der DVD, ergänzt: „Der Niedersachsen-Antrag zeugt von einer erschreckenden Grundrechte-Ignoranz der aktuellen Landesregierung. Sie hat offenbar noch nicht gemerkt, dass angesichts der zunehmenden Digitalisierung in Verwaltung, Wirtschaft und im Alltag Schutzvorkehrungen getroffen werden müssen. Diese sind im bestehenden Datenschutzrecht vorgesehen und erweisen sich weltweit als Vorbild. Die Landesregierung will offenbar, dass Deutschland bei der Digitalisierung weiter den Anschluss verliert. Dazu darf man es nicht kommen lassen. Nur wenn die Bevölkerung darauf vertrauen kann, dass ihre Daten bei den Unternehmen in guten Händen sind – und dazu ist die Umsetzung des Datenschutzes erforderlich, ist eine ausreichende Akzeptanz der Digitalisierung zu erwarten."

Offener Brief des Vereins European Digital Rights[1] vom 15.05.2019 an die Europäische Kommission[2]

Dear Vice-President Andrus Ansip
Dear Commissioner Mariya Gabriel,
Dear Commissioner Vera Jourová,
Dear Chair of the European Data Protection Board Andrea Jelinek,
Dear Chair of the Body of European Regulators for Electronic Communications Jeremy Godfrey,
Dear European Data Protection Supervisor Giovanni Buttarelli,

CC:
Head of Cabinet of Commissioner Gabriel Lora Borissova
Deputy Head of Cabinet of Commissioner Gabriel Carl-Christian Buhr
Wolf-Dietrich Grussmann, DG Connect
Agnieszka Bielinska, DG Connect
Irene Roche-Laguna, DG Connect
Eric Gaudillat, DG Connect
National Regulatory Authorities and Data Protection Authorities of the EEA

We are writing you in the context of the evaluation of Regulation (EU) 2015/2120 and the reform of the BEREC Guidelines on its implementation. Specifically, we are concerned because of the increased use of Deep Packet Inspection (DPI) technology by providers of internet access services (IAS). DPI is a technology that examines data packets that are transmitted in a given network beyond what would be necessary for the provision IAS by looking at specific content from the part of the user-defined payload of the transmission.

IAS providers are increasingly using DPI technology for the purpose of traffic management and the differentiated pricing of specific applications or services (e.g. zero-rating) as part of their product design. DPI allows IAS providers to identify and distinguish traffic in their networks in order to identify traffic of specific applications or services for the purpose such as billing them differently throttling or prioritising them over other traffic.

The undersigned would like to recall the concerning practice of examining domain names or the addresses (URLs) of visited websites and other internet resources. The evaluation of these types of data can reveal sensitive information about a user, such as preferred news publications, interest in specific health conditions, sexual preferences, or religious beliefs. URLs directly identify specific resources on the world wide web (e.g. a specific image, a specific article in an encyclopedia, a specific segment of a video stream, etc.) and give direct information on the content of a transmission.

A mapping of differential pricing products in the EEA conducted in 2018 identified 186 such products which potentially make use of DPI technology. Among those, several of these products by mobile operators with large market shares are confirmed to rely on DPI because their products offer providers of applications



Brussels, 15 May 2019

Dear Vice-President Andrus Ansip
Dear Commissioner Mariya Gabriel,
Dear Commissioner Vera Jourová,
Dear Chair of the European Data Protection Board Andrea Jelinek,
Dear Chair of the Body of European Regulators for Electronic Communications Jeremy Godfrey,
Dear European Data Protection Supervisor Giovanni Buttarelli,

CC:
Head of Cabinet of Commissioner Gabriel Lora Borissova
Deputy Head of Cabinet of Commissioner Gabriel Carl-Christian Buhr
Wolf-Dietrich Grussmann, DG Connect
Agnieszka Bielinska, DG Connect
Irene Roche-Laguna, DG Connect
Eric Gaudillat, DG Connect
National Regulatory Authorities and Data Protection Authorities of the EEA

We are writing you in the context of the evaluation of Regulation (EU) 2015/2120 and the reform of the BEREC Guidelines on its implementation. Specifically, we are concerned because of the increased use of Deep Packet Inspection (DPI) technology by providers of internet access services (IAS). DPI is a technology that examines data packets that are transmitted in a given network beyond what would be necessary for the provision IAS by looking at specific content from the part of the user-defined payload of the transmission.

IAS providers are increasingly using DPI technology for the purpose of traffic management and the differentiated pricing of specific applications or services (e.g. zero-rating) as part of their product design. DPI allows IAS providers to identify and distinguish traffic in their networks in order to identify traffic of specific applications or services for the purpose such as billing them differently throttling or prioritising them over other traffic.

The undersigned would like to recall the concerning practice of examining domain names or the addresses (URLs) of visited websites and other internet resources. The evaluation of these types of data can reveal sensitive information about a user, such as preferred news publications, interest in specific health conditions, sexual preferences, or religious beliefs. URLs directly identify specific resources on the world wide web (e.g. a specific image, a specific article in an encyclopedia, a specific segment of a video stream, etc.) and give direct information on the content of a transmission.

European Digital Rights | 20 Rue Belliard, 1040 Bruxelles, Belgium | Tel. +32 2 274 25 70 | www.edri.org

or services the option of identifying their traffic via criteria such as Domain names, SNI, URLs or DNS snooping.

Currently, the BEREC Guidelines clearly state that traffic management based on the monitoring of domain names and URLs (as implied by the phrase “transport protocol layer payload”) is not “reasonable traffic management” under the Regulation. However, this clear rule has been mostly ignored by IAS providers in their treatment of traffic.

The nature of DPI necessitates telecom expertise as well as expertise in data protection issues. Yet, we observe a lack of cooperation between national regulatory authorities for electronic communications and regulatory authorities for data protection on this issue, both in the decisions put forward on these products as well as cooperation on joint opinions on the question in general. For example, some regulators issue justifications of DPI based on the consent of the customer of the IAS provider which crucially ignores the clear ban of DPI in the BEREC Guidelines and the processing of the data of the other party communicating with the subscriber, which never gave consent.

Given the scale and sensitivity of the issue, we urge the Commission and BEREC to carefully consider the use of DPI technologies and their data protection impact in the ongoing reform of the net neutrality Regulation and the Guidelines. In addition, we recommend to the Commission and BEREC to explore an interpretation of the proportionality requirement included in Article 3, paragraph 3 of Regulation 2015/2120 in line with the data minimization principle established by the GDPR. Finally, we suggest to mandate the European Data Protection Board to produce guidelines on the use of DPI by IAS providers.

Best regards,

Academics and Individuals:
Kai Rannenberg, Chair of Mobile Business & Multilateral Security, Goethe University Frankfurt, Germany Stefan Katzenbeisser, Chair of Computer Engineering, University of Passau, Germany Max Schrems, Privacy Activist, Austria Klaus-Peter Löhr, Professor für Informatik (a.D.), Freie Universität Berlin, Germany Joachim Posegga, Chair of IT-Security, University of Passau, Germany Dominik Herrmann, Chair for Privacy and Security in Information Systems, University of Bamberg, Germany Rigo Wenning, AFS Rechtsanwälte, ERCIM Legal counsel, Vorstand EDV-Gerichtstag, Fitug e.V., France Douwe Korff, Emeritus Professor of International Law, London Metropolitan University, United Kingdom Dr. TJ McIntyre, UCD Sutherland School of Law, United Kingdom Dr Ian Brown, Senior Fellow, Research ICT Africa / CyberBRICS visiting professor, Fundação Getúlio Vargas Direito Rio, Brazil Dr. Jef Ausloos (Institute for Information Law (IViR) -University of Amsterdam), the Netherlands Paddy Leersen LL.M., PhD Candidate University of Amsterdam, Non-Residential Fellow Stanford University Center for Internet & Society, the Netherlands Simone Fischer Hübner, Professor in Computer Science, Karlstad University, Sweden Erich Schweighofer, Head of the Centre for Computers and Law, Department of European, International and Comparative Law, University of Vienna, Austria Prof. Dr.-Ing. Christoph Sorge, Saarland University, Germany Frederik J. Zuiderveen Borgesius, Professor of Law at iCIS Institute for Computing and Information Sciences, Radboud University



A mapping of differential pricing products in the EEA conducted in 2018 identified 186 such products which potentially make use of DPI technology.[1] Among those, several of these products by mobile operators with large market shares are confirmed to rely on DPI because their products offer providers of applications or services the option of identifying their traffic via criteria such as Domain names, SNI, URLs or DNS snooping.[2]

Currently, the BEREC Guidelines[3] clearly state that traffic management based on the monitoring of domain names and URLs (as implied by the phrase "transport protocol layer payload") is not "reasonable traffic management" under the Regulation. However, this clear rule has been mostly ignored by IAS providers in their treatment of traffic.

The nature of DPI necessitates telecom expertise as well as expertise in data protection issues. Yet, we observe a lack of cooperation between national regulatory authorities for electronic communications and regulatory authorities for data protection on this issue, both in the decisions put forward on these products as well as cooperation on joint opinions on the question in general. For example, some regulators issue justifications of DPI based on the consent of the customer of the IAS provider which crucially ignores the clear ban of DPI in the BEREC Guidelines and the processing of the data of the other party communicating with the subscriber, which never gave consent.

Given the scale and sensitivity of the issue, we urge the Commission and BEREC to carefully consider the use of DPI technologies and their data protection impact in the ongoing reform of the net neutrality Regulation and the Guidelines. In addition, we recommend to the Commission and BEREC to explore an interpretation of the proportionality requirement included in Article 3, paragraph 3 of Regulation 2015/2120 in line with the data minimization principle established by the GDPR. Finally, we suggest to mandate the European Data Protection Board to produce guidelines on the use of DPI by IAS providers.

Best regards,

Academics and Individuals:

Kai Rannenberg, Chair of Mobile Business & Multilateral Security, Goethe University Frankfurt, Germany
Stefan Katzenbeisser, Chair of Computer Engineering, University of Passau, Germany
Max Schrems, Privacy Activist, Austria
Klaus-Peter Löhr, Professor für Informatik (a.D.), Freie Universität Berlin, Germany
Joachim Posegga, Chair of IT-Security, University of Passau, Germany
Dominik Herrmann, Chair for Privacy and Security in Information Systems, University of Bamberg, Germany
Rigo Wenning, AFS Rechtsanwälte, ERCIM Legal counsel, Vorstand EDV-Gerichtstag, Fitug

1 See https://epicenter.works/document/1522 page 19-21, 34-35 and 38-40.
2 Cf.
3 BoR (16) 127, paragraphs 69 and 70.

NGOs and NPOs:
European Digital Rights, Europe Electronic Frontier Foundation, International Council of European Professional Informatics Societies, Europe Article 19, International Chaos Computer Club e.V, Germany epicenter.works -for digital rights, Austria Austrian Computer Society (OCG), Austria Bits of Freedom, the Netherlands La Quadrature du Net, France ApTI, Romania Code4Romania, Romania IT-Pol, Denmark Homo Digitalis, Greece Hermes Center, Italy X-net, Spain Vrijschrift, the Netherlands Dataskydd.net, Sweden Electronic Frontier Norway (EFN), Norway Alternatif Bilisim (Alternative Informatics Association), Turkey Digitalcourage, Germany Fitug e.V., Germany Digitale Freiheit, Germany Deutsche Vereinigung für Datenschutz e.V. (DVD), Germany Gesellschaft für Informatik e.V. (GI), Germany LOAD e.V. -Verein für liberale Netzpolitik, Germany

Companies:
Wire Swiss GmbH, Switzerland, Alan Duric, CTO/COO & Co-Founder Research Institute -Digital Human Rights Center, Austria Fédération des Fournisseurs d'Accès Internet Associatifs, France Baycloud Systems, United Kingdom, Mike O'Neill, Director

Übersetzung durch Markus Eßfeld und Frank Spaeing

Diesen Brief schreiben wir[3] mit dem Ziel einer Bewertung der Verordnung (EU) 2015/2120 über Maßnahmen betreffend den Zugang zum offenen Internet und einer Bewertung der Reform der BEREC[4]-Guidelines und deren Umsetzung. Dabei geht es uns insbesondere um die vermehrte Nutzung der sog. Deep Packet Inspection (im Folgenden DPI) der Anbieter von Internetzugangsdiensten (im folgenden IAS-Anbieter). DPI ist ein Verfahren der Netzwerktechnik, das es den Anbietern generell erlaubt Datenpakete über das Erforderliche hinaus zu untersuchen, um damit Erkenntnisse über die eigentlichen Nutzdaten der jeweiligen Kommunikation zu gewinnen und diese ggf. kommerziell zu verwerten.

DPI wird von IAS-Anbietern zunehmend eingesetzt, um den Datenverkehr in Computernetzwerken zu analysieren und ein differenziertes Preissystem für bestimmte Anwendungen und Dienstleistungen[5] als Teil ihres eigenen Produktes einsetzen zu können. DPI erlaubt den IAS-Anbietern, den Datenverkehr zu identifizieren und differenziert betrachten zu können, beispielsweise für die Berechnung bestimmter Dienstleistungen, aber auch für die Priorisierung und Drosselung einzelner Dienste[6].

Die Unterzeichner dieses Briefes möchten auf die verbreitete Praxis der Anbieter hinweisen, Domainnamen oder die Adressen (URL) von besuchten Websites oder anderen Internetquellen zu analysieren. Die Auswertung dieser Daten kann besonders vertrauliche Informationen über einen bestimmten Nutzer enthüllen wie beispielsweise darüber, welche Nachrichtenquellen er bevorzugt, für welche medizinischen Fragen er sich besonders interessiert. Ferner sind Rückschlüsse möglich auf sexuelle Vorlieben oder religiöse Orientierungen. Mit Hilfe der URL können Internetquellen identifiziert werden[7] und direkte Informationen über den Inhalt einer Datenübertragung gegeben werden.

Eine im Jahr 2018 durchgeführte Untersuchung im Europäischen Wirtschaftsraum (EEA) identifizierte 186 Produkte, bei denen die DPI-Technik potentiell eingesetzt wird[8]. Darunter befanden sich zahlreiche Produkte von großen Mobilfunkbetreibern, die mit DPI arbeiten, weil ihr Angebot für Dienste- und Serviceprovider Anwendungen und Dienstleistungen zum identifizieren ihres eigenen Datenverkehrs mit Hilfe von Kriterien wie Domainnamen, SNI[9], URLs oder DNS-Snooping[10] umfasst.

Gegenwärtig legen die BEREC11-Guidelines[12] fest, dass das Monitoring des Datenverkehrs über Domainnamen und URLs[13] keine angemessene Abwicklung des Datenverkehrs[14] darstellt[15]. Diese klare Regelung wird von den IAS-Providern jedoch überwiegend beim Umgang mit Datenverkehr ignoriert.

Die Beurteilung der DPI-Technik erfordert sowohl Sachverstand auf dem Gebiet der Telekommunikation als auch hinsichtlich des Datenschutzes. Allerdings kann man einen Mangel an Kooperation, soweit es um DPI geht, zwischen den jeweiligen nationalen Regulierungsbehörden für Telekommunikation und denjenigen für den Datenschutz feststellen. Das betrifft sowohl die Auseinandersetzung mit den Anbietern bei Verwendung von DPI als auch eine Kooperation der genannten Regelungsbehörden für eine gemeinsame Haltung zu der Frage im Allgemeinen. Beispielsweise halten einige Regulierungsbehörden die Verwendung von DPI für zulässig, wenn der Kunde des IAS-Anbieters dieser zugestimmt habe. Diese Auffassung ignoriert das klare Verbot der DPI gemäß den BEREC-Guidelines. Außerdem wird ignoriert, dass der Datenverkehr des Kunden eines IAS-Anbieters einen Dritten einbeziehen kann, der nie eine Zustimmung zur Nutzung der DPI erteilt hat.

Wegen der Bedeutung des Themas und der besonderen Vertraulichkeit, die der Datenverkehr genießen sollte, möchten wir die EU-Kommission und BEREC dringend bitten, den Gebrauch von DPI Technik und deren Auswirkung auf den Datenschutz sorgfältig zu erwägen, was vor allem im Zusammenhang mit der aktuellen Reform der Netzneutralität[16] und der Guidelines von Bedeutung ist. Darüber hinaus empfehlen wir der EU-Kommission und BEREC die Auslegung des Angemessenheits- bzw. Verhältnismäßigkeitserfordernisses in Art. 3, Abs. 3 der EU-Verordnung 2015/2120 sorgfältig zu erwägen und im Zusammenhang mit dem Grundsatz der Datensparsamkeit zu lesen, wie er in der Datenschutz-Grundverordnung festgeschrieben ist. Abschließend schlagen wir vor, dem Europäischen Datenschutzausschuss das Mandat für die Formulierung von Guidelines zur Nutzung der DPI durch IAS-Anbieter zu erteilen.

1 Internationaler gemeinnütziger Verein nach belgischem Recht, im Folgenden EDRi

2 Im englischen Original sind als Adressaten div. Kommissionsmitglieder u.a. Adressaten namentlich aufgeführt, siehe vorherigen Abdruck in dieser DANA, diese sind in der vorliegenden Übersetzung genauso weggelassen worden wie die unterzeichnenden Personen und Organisationen.

3 Presserechtlich verantwortlich für den Brief ist EDRi, unterzeichnet ist er von zahlreichen natürlichen und juristischen Personen, die mit der Materie befasst sind und sich zu diesem Anliegen äußern.

4 Body of European Regulators for Electronic Communication

5 Z.B. das sog. „zero-rating"

6 Was die Netzneutralität einschränkt.

7 Bis hin zur Identifizierung eines bestimmten Bildes, einem bestimmten Artikel in einer Enzyklopädie oder einer bestimmten Sequenz in einem Video.

8 Siehe https://epicenter.works/document/1522, Seiten 19-21, 34-35 und 38-40.

9 Server Name Indication

10 Angriffe, bei denen mittels IP-Spoofing gefälschte Ressource Records gesendet werden.

11 Body of European Regulators for Electronic Communication

12 BoR (16) 127, Absätze 69 und 70.

13 In den BEREC-Guidelines „transport protocol layer payload" genannt.

14 „is not reasonable traffic management"

15 Siehe Artikel 3 (3) der BEREC-Guidelines

16 Der EU-Verordnung über Maßnahmen für den Zugang zum offenen Internet, VERORDNUNG (EU) 2015/2120

DVD-Presserklärung vom 04.06.2019

#StopSpyingOnUs: Kampagnenstart in 9 EU-Ländern gegen rechtswidrige Online-Werbemethoden

Vierzehn Menschenrechts- und Digitalrechtsorganisationen – darunter auch die Deutsche Vereinigung für Datenschutz e.V. (DVD) – starten heute, koordiniert von Liberties[1], die Kampagne #StopSpyingOnUs[2], indem sie gleichzeitig in neun EU-Ländern bei ihren nationalen Datenschutz-Aufsichtsbehörden Beschwerden gegen illegale Verfahren der Verhaltensorientierten Werbung einreichen. Zu den Ländern, die an der Kampagne teilnehmen, gehören Deutschland, Belgien, Italien, Frankreich, Estland, Bulgarien, Ungarn, Slowenien und die Tschechische Republik. Dies ist die dritte Welle einer Kampagne, die 2018 begann. Die ersten Beschwerden wurden bei den britischen und irischen[3] Datenschutzbehörden eingereicht.

Frank Spaeing, Vorsitzender der DVD: „Mit dieser Kampagne fordern wir die nationalen und europäischen Datenschutzbehörden auf, Ermittlungen gegen einen laufenden, massiven Datenschutzverstoß einzuleiten, der täglich hunderte von Milliarden Mal auftritt und jede Besucherin und jeden Besucher einer Website betreffen kann".

„In dieser Kampagne werden Organisationen und Einzelpersonen zusammenarbeiten, um personenbezogene Daten zu schützen, die ohne unsere Zustimmung weitergegeben werden können, dazu gehören Browser-Historie und Standort, aber auch sexuelle Orientierung und unverwechselbare ID-Codes. Die bei den Datenschutzbehörden eingereichten Beschwerden wenden sich vor allem gegen das System des Real-Time Bidding, durch welches personenbezogene Daten der Nutzer an Hunderte oder Tausende von Unternehmen übertragen werden können. Diese Werbemethode verstößt eindeutig gegen die EU-Datenschutz-Grundverordnung (DS-GVO). Wir haben uns entschieden, eine Kampagne zur Durchsetzung der DSGVO zu starten und sagen, #StopSpyingOnUs „hört auf uns auszuspionieren", so die Liberties Rechtsexpertin Eva Simon.

Zusätzlich zu den offiziellen Beschwerden von Menschenrechts- und Digitalrechtsorganisationen[4] haben Liberties unsere Partner in mehreren Sprachen Musterbeschwerden für Personen vorbereitet, die sich der Kampagne #StopSpyingOnUs anschließen möchten. In einer Reihe von Ländern können Interessierte den Forderungen Nachdruck verleihen, indem sie mit einem auf Liberties.eu verfügbaren Musterbrief einfach eine Beschwerde an ihre nationalen Datenschutzbehörden richten.

„Wir wollen, dass die Stimme der Menschen gehört wird und deshalb geben wir ihnen alle Instrumente an die Hand, die sie brauchen, um die Verletzung ihrer Rechte im Ökosystem der Online-Werbung zu verhindern. Wenn unsere persönlichen Daten ohne Erlaubnis weitergegeben werden, sollten wir sagen können, dass uns das nicht passt und in der Lage sein dafür zu sorgen, dass das aufhört.", sagt Orsolya Reich, Advocacy Officer bei Liberties.

Diese Online-Werbemethode wird von mehreren Schlüsselunternehmen im digitalen Bereich, wie z.B. Google, genutzt, was dazu führt, dass eine riesige Anzahl von Personen diesem Datenaustausch ausgesetzt ist. So ist beispielsweise Googles DoubleClick (vor Kurzem umbenannt in „Authorized Buyers") auf 8,4 Millionen Websites aktiv und übermittelt personenbezogene Daten über Besucher dieser Websites an über 2.000 Unternehmen. Deshalb sagen wir, #StopSpyingOnUs[5], „hört auf uns auszuspionieren".

1 https://www.liberties.eu/de

2 https://www.liberties.eu/de/campaigns/stopspyingonus-fixad-tech-kampagne/307

3 https://fixad.tech/

4 Die deutschsprachige Datenschutzbeschwerde finden Sie unter: https://www.datenschutzverein.de/wp-content/uploads/2019/06/Beschwerde_verhaltensbasierte_Werbung_04062019.pdf

5 https://www.liberties.eu/de/campaigns/stopspyingonus-fixad-tech-kampagne/307

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Bundeskartellamt geht gegen Datenmacht Facebooks vor

Die deutschen Wettbewerbshüter des Bundeskartellamts fordern, dass Facebook sein Geschäftsmodell fundamental ändert. Der US-Konzern hat demnach ein Jahr Zeit, die Datensammlung umzustellen. Facebook soll die Daten aus unterschiedlichen Plattformen nur noch zusammenführen dürfen, wenn die Nutzenden ausdrücklich zustimmen. Das Kartellamt teilte in Bonn am 07.02.2019 mit, dass es nach einer dreijährigen Prüfung zu dem Ergebnis gekommen ist, dass der US-Konzern seine Marktmacht missbrauche, um Daten seiner Nutzenden zu sammeln. Behördenchef Andreas Mundt begründete: „Die Nutzer haben keine Wahl, ob sie der Datensammlung zustimmen oder nicht." In Zukunft soll Facebook seinen Mitgliedern eine explizite Wahl lassen, ob die Daten, die auf Facebook.com, anderen Diensten wie WhatsApp, Instagram und Websites mit integriertem Facebook-Plugin gesammelt wurden, wieder unter der einheitlichen Facebook-ID zusammengeführt werden dürfen. Es handelt sich hier um den ersten Fall, in dem das 2017 novellierte deutsche Kartellrecht auf einen großen Digitalkonzern angewendet wird. Das Gesetz gegen Wettbewerbsbeschränkungen (GWB) war geändert worden, um die Internetökonomie mit Firmen wie Google, Uber oder Amazon zu erfassen, bei der KundInnen nicht (nur) mit Geld, sondern insbesondere mit ihren Daten bezahlen.

Das Kartellamt geht davon aus, dass Facebook den Markt sozialer Netzwerke beherrscht. Mit 23 Mio. Nutzenden täglich komme der Konzern in Deutschland auf einen Marktanteil von 95%. Andere soziale Netzwerke wie LinkedIn, Xing oder YouTube befriedigten andere Bedürfnisse und seien deshalb insofern nicht relevant. 40 bis 60 Mio. Menschen nutzen nach Angaben des Kartellamtes hierzulande täglich Whatsapp, bei der Fotoplattform Instagram sind es demnach 10 bis 20 Mio. täglich Nutzende. Facebook soll innerhalb von vier Monaten ein Konzept vorlegen, wie es künftig bei der Zusammenführung von Daten vorgehen wolle. Innerhalb eines Jahres soll das neue Regime dann umgesetzt sein. Mundt zeigte sich zunächst optimistisch, dass Facebook sich der Entscheidung seiner Behörde beugen werde: „Ich bin sicher, dass sich viele Wettbewerbsbehörden dieses Verfahren sehr genau ansehen werden." Zudem könne seine Behörde Bußgelder bis zu zehn Millionen Euro verhängen, die auch monatlich verhängt werden könnten, wenn sich Facebook dauerhaft weigere den Vorgaben der Behörde nachzukommen.

Der Behördenchef sparte nicht mit Kritik am Geschäftsmodell von Facebook sowie anderer Internetunternehmen: „Diese Unternehmen überziehen uns mit einer neuen wirtschaftlichen Ordnung." Über Lock-In- und Netzwerk-Effekte habe Facebook in den vergangenen Jahren einen gewaltigen Datenschatz angehäuft, der den Nutzenden keine Wahl lasse, den Facebook-Account stillzulegen, ohne eine Einschränkung wahrzunehmen.

Bei seiner Entscheidung stützt sich das Bundeskartellamt im Wesentlichen auch auf die Datenschutz-Grundverordnung (DSGVO). Die Behörde konnte keine Rechtfertigung finden, warum Facebook in dem heutigen Ausmaß Nutzerdaten sammeln könne. Mundt wehrte sich dabei gegen den Vorwurf, dass die Wettbewerbsbehörde ihre Kompetenzen überschreite: „Wie bitte soll ein Datenschützer prüfen, ob eine Einwilligung freiwillig ist oder nicht freiwillig ist, weil das Unternehmen marktbeherrschend ist?"

Facebook kündigte an, gegen die Entscheidung Rechtsmittel einzulegen. Sollte das Oberlandesgericht Düsseldorf eine einstweilige Verfügung zugunsten von Facebook verhängen, würden die Auflagen des Kartellamtes zunächst nicht wirksam werden. Das Unternehmen warf der Behörde vor, die marktbeherrschende Stellung falsch diagnostiziert zu haben: „Wir haben in Deutschland einen harten Wettbewerb mit anderen Diensten, doch das Bundeskartellamt hält es für irrelevant, dass unsere Apps mit YouTube, Snapchat, Twitter und vielen anderen Wettbewerbern um die Aufmerksamkeit der Nutzer konkurrieren". Dies wurde vom Bundeskartellamt zurückgewiesen: „Es gibt kein soziales Netzwerk, das Facebook auch nur nahe kommt." Damit stehe Facebook auch in der Pflicht, seine Angebote nicht unter unangemessenen Konditionen anzubieten. Angesichts der umfassenden Datenprofile sei dies aber nicht gewährleistet. Berichte über nachlassende Facebook-Nutzung könne seine Behörde nicht bestätigen.

Facebook argumentiert außerdem, es sei durchaus im Sinne der Nutzenden, Daten zu sammeln, um den Missbrauch von Nutzerkonten zu verhindern, z. B. für „Terrorismus, Kindesmissbrauch oder die Manipulation von Wahlen". Tatsächlich gesteht das Kartellamt zu, dass Facebook in drängenden Sicherheitsfragen auch künftig Daten seiner Dienste zusammenführen dürfe. Facebook macht geltend, dass das Kartellamt sein Mandat überschreitet. Für den Datenschutz des Unternehmens sei die irische Datenschutzbehörde zuständig, da der Konzern seine Europazentrale in Dublin hat. Die Iren gehen erfahrungsgemäß mit Facebook freundlicher um als die Aufsichtsbehörden auf dem Festland. Mundt erwiderte, ihm gehe es nicht umfassend um den Datenschutz, sondern nur, soweit bei Verstößen die Marktmacht missbraucht wird. Das Kartellamt habe jedenfalls intensiv mit ausländischen Datenschutzbehörden zusammengearbeitet: „Da gab es keinerlei Wi-

derstand." So begrüßte auch der neue Bundesdatenschutzbeauftragte Ulrich Kelber die Kartellentscheidung.

Der Behauptung Facebooks, es halte sich an die DSVGO, akzeptiert das Bundeskartellamt nicht. Zwar könnten Nutzende inzwischen in den Facebook-Einstellungen personalisierte Werbung deaktivieren; dies ändere jedoch nichts an der umfassenden Datenerhebung. Etwa ein Drittel der mehr als 300-seitigen Entscheidung des Bundeskartellamts befasst sich mit den Details des Datenschutzrechts. Mit einer Pro-Forma-Zustimmung, die an die unbeschränkte Nutzung der Plattform gekoppelt ist, will es das Bundeskartellamt nicht bewenden lassen. Das Unternehmen müsse in seinem Konzept darlegen, in welcher Form es die Zustimmung künftig erheben werde.

Der Vorstand des Verbraucherzentrale Bundesverbands, Klaus Müller, begrüßte die Entscheidung: „Der Datensammelwut des Unternehmens wird nun zum Schutz von Verbraucherinnen und Verbrauchern auch mit Mitteln des Kartellrechts begegnet." Der Digitalverband Bitkom kritisierte hingegen, dass die Regulierung von Facebook negative Folgen für kleine Firmen und Verlage haben könnte, denn sie profitierten vom „Gefällt-mir-Button" (Kleinz, Bundeskartellamt: Facebook soll angehäufte Daten entbündeln, www.heise.de 07.02.2019, Kurzlink: https://heise.de/-4300461; Brühl/Müller, Kartellamt bremst Facebook, SZ 08.02.2019, 1; Müller, Bonner Brandmauer, SZ 08.02.2019, 2).

Bund

BND soll mehr Befugnisse erhalten

Gemäß einem Referentenentwurf aus dem Kanzleramt und dem Bundesinnenministerium soll der deutsche Auslandsgeheimdienst, der Bundesnachrichtendienst (BND), künftig zusätzliche Befugnisse erhalten, z. B. Handys von Deutschen ausspähen und V-Leute vor der Staatsanwaltschaft schützen. Seit März 2019 diskutieren die Koalitionspartner von Union und SPD einen Gesetzentwurf, wonach der BND auch im Inland eine stärkere Rolle spielen soll. Der BND soll künftig „informationstechnische Systeme" von natürlichen und juristischen Personen auch im Inland infiltrieren und ausforschen dürfen. Voraussetzung ist, dass eine solche Ausforschung mit Trojanersoftware der „Erkennung und Begegnung" von bestimmten Gefahren und Straftaten „dient". Diese Gefahren und Straftaten werden im Einzelnen aufgelistet. Dabei geht es um Terrorismus, Menschenschmuggel, aber auch um Bedrohungen für die IT-Sicherheit. Dies wird von dem Mainzer Rechtsprofessor Matthias Bäcker kritisiert: „Das kann viel bedeuten." Da der BND keinen konkreten Anfangsverdacht vorweisen müsse, sei die Schwelle für den Einsatz des BND-Trojaners recht niedrig – niedriger als bei der Polizei. Im Ausland und gegenüber Ausländern soll der BND Online-Durchsuchungen frei einsetzen können, um „Erkenntnisse von außen- und sicherheitspolitischer Bedeutung zu gewinnen".

Nach den Plänen der Bundesregierung soll die Trennung zwischen Polizei und Geheimdiensten weiter aufgeweicht werden. So soll der BND künftig für die deutschen Landespolizeien „verstetigte Amtshilfe" bei Online-Durchsuchungen leisten: „Die ersuchende Behörde trägt gegenüber dem Bundesnachrichtendienst die Verantwortung für die Rechtmäßigkeit der durchzuführenden Maßnahme", so der Gesetzentwurf. Der BND soll dabei nur die technische Ausführung übernehmen. Er soll die gewonnenen Daten an die Polizei weiterreichen, ohne selbst von ihnen Kenntnis zu nehmen. Wenn es aber zum Beispiel um internationalen Terrorismus geht, für den der BND selbst mit zuständig ist, soll der BND die Daten „für eigene Zwecke weiterverarbeiten" dürfen. Matthias Bäcker: „Die polizeiliche Tätigkeit ist ohnehin stärker der nachrichtendienstlichen Tätigkeit angeglichen worden in den vergangenen Jahrzehnten. Nun lässt man gleich die Fachleute ran."

V-Leuten, also Informanten für den BND, die z. B. für ein russisches Staatsunternehmen oder die iranische Botschaft in Deutschland arbeiten, für Waffenschieber oder internationale Finanziers bei dunklen Geschäfte, soll der BND bessere Anreize bieten können: Bislang durfte der BND nicht viel bezahlen. Die Vorgabe lautete, dass der Lohn für V-Leute („angebahnte und geführte Personen" im BND-Jargon) nie so hoch sein durfte, dass er den größten Teil des Einkommens ausmacht. Der Grund: Wenn die Existenz eines Menschen davon abhängt, dass er dem Dienst immer wieder interessante Dinge zu erzählen weiß, dann wächst die Versuchung, irgendwann auch Geschichten zu erfinden. Das war eine Lehre aus dem NSU-Debakel. Nun soll diese Vorgabe gelockert werden. Der BND soll frei sein zu bezahlen, was er möchte. Zur Begründung heißt es, in wirtschaftlich ärmeren Krisenländern seien auch 50 Euro im Monat schnell mal ein Professorengehalt.

Zudem sollen Kriminelle, die dem BND Informationen zustecken, künftig stärkeren Schutz vor Strafverfolgung erwarten können. Wenn der BND mitbekommt, dass seine V-Leute in Deutschland Straftaten begehen, dann soll er dies nicht zwingend anzeigen müssen. Stattdessen darf darüber „die Amtsleitung" des BND frei entscheiden. Bekommt die V-Person dennoch Ärger mit Polizei oder Staatsanwaltschaft, kann sich der BND auch schützend vor sie stellen. Bislang lautete das Prinzip: Die Staatsanwaltschaft „kann" bei V-Leuten des BND von einer Verfolgung absehen, vorausgesetzt, die Tat wiegt nicht zu schwer. Künftig soll es heißen: Die Staatsanwaltschaft „soll" von der Verfolgung absehen. Der an der Universität Köln lehrende Nachrichtendienstrechtler Nikolaos Gazeas kommentiert: „Das heißt, es wird in aller Regel ein Deckel draufgemacht." Der BND könne dann künftig fast immer mit Erfolg bei der Justiz intervenieren. Der BND-Präsident soll schließlich im Einzelfall auch verurteilte Verbrecher als V-Leute anwerben können, solange die Tat nicht Mord, Totschlag oder ein anderes Tötungsdelikt war. Hier übernähme der BND den rechtlichen Standard für V-Leute, der bisher schon beim Verfassungsschutz gilt.

Im Koalitionsvertrag von Union und SPD steht, dass jede Ausweitung von Geheimdienstbefugnissen auch eine „entsprechende Ausweitung der parlamentarischen Kontrolle" erfordert. In dem vorgelegten Gesetzentwurf findet sich dazu nichts (Steinke, Macht hinter Mauern, SZ 30./31.03.2019, 7; siehe

dazu auch den Artikel von Krempl, Seehofers Geheimdienstgesetz: Die Abrissbirne für die Grundrechte, www.heise.de 19.04.2019, Kurzlink: https://heise.de/-4401986).

Bund

TKG-Änderung geplant für sichereres 5G

Angesichts der Sicherheitsdebatte über den Netzausbau bei der neuen Mobilfunkgeneration 5G und den chinesischen Netzausrüster Huawei plant die Bundesregierung eine Änderung des Telekommunikationsgesetzes (TKG). Innenminister Horst Seehofer (CSU) kündigte in einem Gespräch mit Innenpolitikern der Regierungskoalition am 12.02.2019 in Berlin an, dass der § 109 TKG geändert werden soll. Damit wolle die Regierung aber nicht Huawei vom Markt fernhalten; es gehe um bessere Kontrolle. Demnach sollen künftig die Lieferanten der Netzbetreiber ihre Produkte unter Sicherheitsaspekten zertifizieren lassen und Sicherheitsgarantien abgeben. Diese Auflagen würden dann für alle gelten. In § 109 TKG werden Auflagen für Netzbetreiber und andere Anbieter von Telekommunikationsdiensten aufgeführt. Die Unternehmen müssen unter anderem dafür sorgen, dass ihre Netze und Dienste gegen Missbrauch und Störungen angemessen gesichert sind, um etwa das Fernmeldegeheimnis und sensible Daten zu schützen.

Huawei ist weltweit Marktführer bei der Mobilfunktechnik. Die Produkte des chinesischen Herstellers werden von nahezu allen westlichen Netzbetreibern eingesetzt. Im Hinblick auf den Netzausbau mit 5G wächst bei Regierungen die Sorge, dass die Technik von Huawei ein Sicherheitsrisiko für eine kritische Infrastruktur bedeutet. Das chinesische Nachrichtendienstgesetz könnte Huawei dazu zwingen, sensible Informationen mit dem Geheimdienst zu teilen. Bisher ist nicht bekannt, ob das schon einmal vorgekommen ist. Auch Spekulationen über mögliche Hintertüren oder „Kill-Switches" in der Huawei-Technik entbehrten bisher jeden Nachweises. Huawei weist alle Vorwürfe zurück. Vor einem Beschluss zur Änderung des deutschen TKG soll mit den betroffenen Unternehmen gesprochen werden. Dabei gehe es um Kosten, Machbarkeit und Sicherheitsvorkehrungen. Das Gesetz ist nicht schon zur 5G-Auktion anwendbar, die seit März 2019 stattfindet.

Die US-Regierung hatte in den vorangegangenen Monaten bei befreundeten Regierungen darauf gedrungen, beim 5G-Ausbau auf Huawei zu verzichten. Die großen US-Netzbetreiber setzen die chinesische Technik nicht ein. Viele kleinere, regionale US-Carrier haben ihre Netze aber mit Komponenten von Huawei oder ZTE gebaut. Sie würde ein Bann für chinesische Technik hart treffen. US-Präsident Donald Trump will eine entsprechende Verordnung erlassen. Aufgrund dieser Verordnung müsste das Handelsministerium amerikanischen Unternehmen den Einkauf von Netztechnik untersagen, die ein Sicherheitsrisiko darstellt (Briegleb, Seehofer will wegen Huawei das TKG ändern, www.heise.de 12.02.2019, Kurzlink: https://heise.de/-4307334).

Bund

Schutz von Geschäftsgeheimnissen und Whistleblowing

Ohne Aussprache billigte der Bundesrat am 12.04.2019 nach dem Bundestag im März abschließend einen Gesetzentwurf, mit dem die Politik eine EU-Richtlinie von 2016 zum Schutz von Geschäftsgeheimnissen in nationales Recht umsetzen will. Für Geschäftsgeheimnisse, die etwa durch „eigenständige Entdeckung oder Schöpfung" erlangt werden können, gilt dann ein einheitlicher Mindestschutz ähnlich wie bei Urheberrechten, Patenten oder Marken. Inhabern solcher Ansprüche wird es ermöglicht, Rechtsverletzer „auf Beseitigung der Beeinträchtigung und bei Wiederholungsgefahr auch auf Unterlassung in Anspruch" zu nehmen. Sie dürfen darauf hinwirken, dass erlangte Dokumente, Gegenstände, Materialien, Stoffe oder elektronische Dateien vernichtet oder herausgegeben werden und rechtsverletzende Produkte zurückgerufen oder zerstört werden. Eine Information gilt nur dann als Geschäftsgeheimnis, wenn der Antragsteller ein „berechtigtes Interesse" an einem entsprechenden Schutz geltend machen kann. Wer eine Straftat oder einen Rechtsverstoß durch staatlich unterstützte Geheimniskrämerei vertuschen will, hat damit keine guten Karten.

Bei WhistleblowerInnen oder JournalistInnen greift eine Ausnahmeklausel: Sie werden nicht mehr per se als Rechtsverletzer oder Beihelfer angesehen, wenn sie Geschäftsgeheimnisse publik machen. Sie dürfen eine „rechtswidrige Handlung" oder ein berufliches oder sonstiges Fehlverhalten aufdecken, wenn die „Erlangung, Nutzung oder Offenlegung" eines geschützten Geheimnisses „geeignet ist, das allgemeine öffentliche Interesse zu schützen".

Das Whistleblower-Netzwerk erhofft sich von dem Gesetz ein Signal an die Strafverfolgungsbehörden, ein Ermittlungsverfahren bei klarer Sachlage von vornherein auszuschließen. Die staatliche Transparenz könnte unter der Initiative aber leiden. So sah etwa das Bundesverkehrsministerium kein „berechtigtes Interesse" der Öffentlichkeit an Details aus den Vereinbarungen für die Lkw-Maut. Es will weite Teile des Toll-Collect-Vertrags als Geschäftsgeheimnis eingestuft wissen (Krempl, Bundesrat stimmt für mehr Schutz von Geschäftsgeheimnissen und Whistleblowern, www.heise.de 12.04.2019, Kurzlink: https://heise.de/-4398431; zum Schutz von Whistleblowern nach EU-Recht s. u. S. 97).

Bund

PNR-Datenabgleich höchst fehlerhaft

Seit 2018 erfasst das Bundeskriminalamt (BKA) die Daten aller Flugpassagiere, die in Deutschland starten oder landen. So sollen gesuchte Kriminelle und Straftatverdächtige identifiziert und polizeilich beobachtet werden können. Tatsächlich lieferte das System in den ersten Betriebsmonaten jede Menge Treffer. Gemäß der Antwort der Bundesregierung auf eine kleine Anfrage des Abgeordneten Andrej Hunko

(Die Linke) waren jedoch die meisten Trefferdaten unbrauchbar. Auf jede korrekte Verdachtsmeldung kamen mehr als 400 falsche Treffer. Im sogenannten Passenger Name Record (PNR) speichern die Fluglinien Daten zu ihren Passagieren. Die Datensätze enthalten etwa Datum, Uhrzeit, Start- und Zielflughafen der gebuchten Verbindung sowie Name, Anschrift und Zahlungsdaten des Reisenden. Das Fluggastdatengesetz verpflichtet die Airlines, diese Informationen an das BKA weiterzugeben. Dort ist eine Software im Einsatz, welche die Daten mit Fahndungslisten abgleicht.

Künftig sollen die PNR-Daten nicht nur nach gesuchten Personen durchforstet werden, sondern auch nach verdächtigen Mustern, die auf eine für die Zukunft geplante Straftat hinweisen. Das Fluggastdatengesetz gilt als erster großangelegter Einsatz von Predictive Policing in Deutschland. Solche Vorhersagemodelle sind naturgemäß schwierig und grundsätzlich fehlerbehaftet. Doch offenbar hat das BKA schon große Probleme mit der Umsetzung des vorherigen, vergleichsweise trivialen Schritts: dem Abgleich der PNR-Daten mit den Fahndungslisten der Polizeibehörden. Die Software liefert bisher in der großen Mehrheit falsche Treffer, die anschließend händisch von BeamtInnen wieder aussortiert werden müssen.

Dabei sind zwei Arten von Fehlern zu unterscheiden: Die eine Art betrifft Verdächtige, die nicht als solche erkannt werden. Ihre Zahl lässt sich regelmäßig nicht ermitteln. Die zweite Art von Fehlern betrifft Personen, die fälschlicherweise als Verdächtige eingestuft werden. Im Polizeibereich sind diese sogenannten falsch positiven Treffer besonders heikel, da auf diesem Wege Menschen zu Unrecht ins Visier der Sicherheitsbehörden geraten. Linken-Politiker Hunko sprach von „aberwitziger Überwachung“: „Die Bundesregierung kann nicht belegen, dass mit der Fluggastdatenspeicherung Straftaten aufgeklärt oder Gefahren verhindert werden.“ Zwischen der Inbetriebnahme am 29.08.2018 und dem 31.03.2019 hatten die Fluglinien Daten von 1,2 Mio. Passagieren ans BKA weitergegeben. Die Software fand darin 94.098 „technische Treffer“. Jeder einzelne davon wurde von einer BeamtIn händisch überprüft. In 277 Fällen stellte sich der Verdacht als begründet heraus. In 93.821 Fällen handelte es sich dagegen um ein Fehlurteil der Software. Daraus ergibt sich eine Falsch-positiv-Rate von 99,7%.

Das Bundesinnenministerium (BMI) begründet die hohe Fehlerrate damit, dass häufig Menschen markiert würden, die den gleichen Namen wie auf der Fahndungsliste stehende Personen haben. Diese Fehlerquelle ließe sich eindämmen, wenn neben dem Namen auch das Geburtsdatum abgeglichen würde. Dieses wird jedoch mit den Fluggastdaten nicht übermittelt. Ein Sprecher des Innenministeriums sagte, man sammle derzeit Erfahrungen und werde dann auf EU-Ebene überprüfen, ob man das Verfahren verbessern kann. Laut BMI sind etwa 40 BeamtInnen im 24/7-Schichtdienst mit der Überprüfung der technischen Treffer beschäftigt. Insgesamt sieht die Bundesregierung für Aufbau und Betrieb der Fluggast-Datenbank mehr als 500 Planstellen in verschiedenen Behörden vor. Die Daten der 277 überprüften Treffer wurden an BKA und Zoll weitergegeben – zur „Umsetzung der Fahndungsmaßnahme“, also etwa Festnahmen oder Durchsuchungen. Die Einträge der Fluggast-Datenbank werden nach einem halben Jahr anonymisiert und nach fünf Jahren vollständig gelöscht (Endt, Überwachung von Flugpassagieren liefert Fehler über Fehler, www.sueddeutsche.de 24.04.2019).

Bund

Regierung plant Implantateregister

Die Bundesregierung plant ein Gesetz für ein deutsches Implantateregister. Die Datenbank soll helfen, implantierte Medizinprodukte wie Herzschrittmacher, Brustimplantate oder künstliche Hüftgelenke besser zu kontrollieren. Ende November 2018 hatte ein Konsortium von Medien (International Consortium of Investigative Journalists – ICIJ) nach weltweiten Recherchen auf Probleme mit Medizinprodukten aufmerksam gemacht und in den „Implant Files“ gefährliche Missstände aufgedeckt. Schon seit Jahren wird über ein Implantateregister nachgedacht. Die Implant-Files haben nun offenbar das Gesundheitsministerium darin bestärkt „zu prüfen, wie das bestehende System der Zulassung und Überwachung von Medizinprodukten verbessert werden kann“.

Gemäß dem Gesetzentwurf soll das Implantateregister beim Deutschen Institut für Medizinische Dokumentation und Information (Dimdi) eingerichtet werden, das dem Bundesgesundheitsministerium untersteht. Dort soll gespeichert werden, welchen PatientInnen wann und wo welches Implantat eingesetzt und evtl. auch wieder herausoperiert wurde. Auf lange Sicht lässt sich damit auch feststellen, welche Implantate besonders häufig zu Verletzungen oder gar Todesfällen führten. Künftig soll damit auch vermieden werden, „dass in einigen Gesundheitseinrichtungen noch Produkte implantiert werden, die anderswo schon als problematisch aufgefallen sind“, so die Gesetzesbegründung. Auch bei Rückrufen fehlerhafter Prothesen oder Schrittmacher ist ein Implantateregister hilfreich. Bislang müssen Hersteller Kliniken und Ärzte informieren, die dann wiederum ihre PatientInnen benachrichtigen sollen. Wie die Implant-Files-Recherchen zeigten, haben PatientInnen in der Vergangenheit aber oft wochen- oder gar monatelang nicht erfahren, dass ein Implantat, das sie in ihrem Körper tragen, fehlerhaft ist.

PatientInnen hatten in Deutschland bislang wenige Möglichkeiten, sich über womöglich fehlerhafte Medizinprodukte zu informieren. So sammelt das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) zwar die Probleme, die Ärzte und Hersteller im Zusammenhang mit Implantaten melden, aber die Datenbank ist – anders als z. B. in den USA – nicht öffentlich einsehbar. Das BfArM hat bislang auch die Auskunft darüber verweigert, welche fehlerhaften Implantate in der Vergangenheit in der Bundesrepublik zu den meisten Todesfällen geführt haben. Das Implantateregistergesetz soll 2020 in Kraft treten. Gemäß Minister Jens Spahn (CDU) wird der Aufbau des Registers voraussichtlich drei bis fünf Jahre dauern (Ludwig/Obermaier, Mehr Transparenz bei Implantaten, SZ 01.02.2019, 6).

Bundesweit

Erste Bußgeldverfahren in Deutschland

Bundesweit ergingen bis Mitte Januar 2019 in 41 Fällen Bußgeldbescheide wegen Verstößen gegen die Datenschutz-Grundverordnung (DSGVO). Das erste DSGVO-Bußgeld kassierte wohl ein soziales Netzwerk in Höhe von 20.000 €. Hacker hatten bei der Chat-Plattform Knuddels die Passwörter, E-Mail-Adressen und Pseudonyme von 330.000 Nutzenden abgegriffen und im Internet veröffentlicht. Die verhältnismäßig milde Strafe war auf die Kooperationsbereitschaft mit der zuständigen Datenschutzbehörde zurückzuführen.

Gemäß einer journalistischen Umfrage unter den Datenschutzbeauftragten der Länder ergingen bundesweit bis dahin in 41 Fällen Bußgeldbescheide. Die Strafen kamen recht schnell, denn die Ermittlungsverfahren dauern in der Regel einige Monate. Die Behörden teilten zudem mit, dass „sehr viele" weitere Bußgeldverfahren laufen. Die EU-Datenschutzgrundverordnung gilt seit dem 25.05.2018 für die Verarbeitung, Speicherung und Weitergabe personenbezogener Daten durch öffentliche Stellen und private Firmen (Anger/Neuerer, Behörden verhängen erste Bußgelder wegen Verstößen gegen DSGVO, www.handelsblatt.com 18.01.2019).

Bundesweit

Bitkom-Umfrage zu Datenschutzbeauftragten in Wirtschaftsunternehmen

Gemäß einer repräsentativen Unternehmensbefragung im Auftrag des Digitalverbands Bitkom hat derzeit fast jedes dritte Unternehmen in Deutschland (31%) eine Vollzeitstelle für Mitarbeitende eingeplant, die sich hauptsächlich mit Datenschutz befasst. Sechs von zehn Unternehmen (59%) haben dafür weniger als eine Vollzeitstelle zur Verfügung. Susanne Dehmel, Mitglied der Bitkom-Geschäftsführung für Recht und Sicherheit, erklärte: „Mit der Datenschutzgrundverordnung ist der Aufwand für viele Unternehmen enorm gestiegen. Wer qualifiziertes Personal finden konnte, hat dies auch eingestellt. Beim Datenschutz herrscht jedoch deutschlandweit Fachkräftemangel."

Nur wenige Unternehmen setzen auf mehr als eine Vollzeitstelle für Datenschutzthemen. 4% haben demnach bis zwei Vollzeitäquivalente dafür eingeplant, nur 1% bis drei Vollzeitäquivalente. Vor allem große Betriebe beschäftigen mehrere Datenschutzexperten. Jedes dritte Unternehmen ab 500 Mitarbeitende (35%) hat dafür bis zu vier Stellen vorgesehen, jedes Vierte (28%) vier oder mehr Vollzeitarbeitsplätze. Laut Dehmel war das Jahr 2018 für viele Kanzleien und Rechtsberater mit Datenschutz-Knowhow sehr arbeitsintensiv. Weiterhin seien viele Unternehmen damit beschäftigt, ihre Geschäftsprozesse an die DSGVO-Vorgaben anzupassen. Die Umfrage wurde vom BitkomResearch im Auftrag des Bitkom durchgeführt. Dabei wurden 502 für den Datenschutz verantwortliche Personen (Betriebliche Datenschutzbeauftragte, Geschäftsführer, IT-Leiter) von Unternehmen aller Branchen ab 20 Mitarbeitern in Deutschland telefonisch befragt.

Bitkom kritisierte die schon seit Längerem geplante E-Privacy-Verordnung, die die DSGVO im Bereich der elektronischen Kommunikation ergänzen soll: „Mit dem derzeitigen Entwurf gefährdet die E-Privacy-Verordnung Softwareupdates und schränkt werbebasierte Geschäftsmodelle im Internet ein." Auch hinsichtlich der in der EU verhandelten so genannten E-Evidence-Verordnung, mit welcher der Zugriff von Strafverfolgungsbehörden auf elektronische Beweismittel erleichtert werden soll, sieht Bitkom Nachbesserungsbedarf. Strafverfolgungsbehörden eines Mitgliedsstaates könnten demnach von Providern verlangen kurzfristig elektronische Beweise herauszugeben, auch wenn diese in einem anderen Mitgliedsstaat ansässig sind. Dehmel: „Private Provider sollten keine Grundrechtsprüfungen vornehmen, ohne dass nationale Behörden miteinbezogen werden" (Datenschutzexperten sind die Ausnahmen in Unternehmen, www.bitkom.org, 25.01.2019).

Bundesweit

Binder Datenschutzbeauftragter mehrerer Rundfunkanstalten

Die Aufsichtsgremien der öffentlich-rechtlichen Rundfunkanstalten BR, SR, WDR, ZDF und Deutschlandradio haben Dr. Reinhart Binder zum gemeinsamen hauptamtlichen Rundfunkdatenschutzbeauftragten ihrer Häuser berufen. Gemäß einer Mitteilung des BR-Rundfunk- und Verwaltungsrats beaufsichtigt Binder seit dem 01.01.2019 als unabhängige Behörde die betrieblichen Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten. Binder ist Jurist mit spezifischen rundfunkrechtlichen Kenntnissen. Er war unter anderem zeitweilig Vorsitzender des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio und hat damit Erfahrungen im Datenschutz.

Nach Inkrafttreten der europäischen Datenschutz-Grundverordnung (DSGVO) waren bis zum 25.05.2018 Vorgaben in den einschlägigen Staatsverträgen bzw. Landesgesetzen umzusetzen. Anschließend haben die insoweit jetzt gesetzlich zuständigen Aufsichtsgremien des öffentlich-rechtlichen Rundfunks auch die Regelungen zur datenschutzrechtlichen Aufsicht konkretisiert. Die Aufsichtsgremien der genannten fünf Rundfunkanstalten haben sich für eine Kooperation bei der Datenschutzbehörde entschieden. Mit der Errichtung und der organisatorischen Angliederung an die Geschäftsstellen der Aufsichtsgremien der Rundfunkanstalten soll die in der DSGVO geforderte Unabhängigkeit der Datenschutzaufsicht gestärkt und eine größere Arbeitseffizienz ermöglicht werden. Vor Ablauf der Amtszeit des Rundfunkdatenschutzbeauftragen wollen die zuständigen Aufsichtsgremien der beteiligten Anstalten die Kooperation bei der Datenschutzaufsicht evaluieren (Öffentlich-Rechtliche berufen gemeinsamen Rundfunkda-

tenschutzbeauftragten, www.infosat.de 02.01.2019).

Bundesweit

Illegale Telefonmitschnitte im Volkswagen-Konzern

Wolfgang Hatz, der ehemalige Chef-Motoren-Entwickler des Volkswagen-Konzerns, stürzte durch den Diesel-Skandal tief ab. Hatz wurde schon wenige Tage nach Bekanntwerden der Vorwürfe als Porsche-Vorstand beurlaubt. Derart unfreiwillig frei gestellt, rief er mehrere Konzern-Manager an, zeichnete die Gespräche ohne deren Wissen auf und übergab die Mitschnitte seinem Anwalt. Betroffen sind der damalige Volkswagen-Chef Matthias Müller, Porsche-Boss Oliver Blume und Vorstandskollege Michael Steiner. Wie aus dem Hause Porsche zu hören ist, sind die drei Herren nicht begeistert angesichts des Vertrauensbruchs, zumal das Handelsblatt genüsslich aus den Protokollen zitierte und es in den Gesprächen explizit um die „Bescheiß-Software" ging. „Mia, i moan, i muaß, i muaß, i wui da do nix vormacha", soll Matthias Müller auf gut bayerisch gesagt haben, „äh, mia kennan nicht gegen den Aufsichtsrat von VW entscheiden". Hatz habe in den Telefonaten stets betont, dass er keinerlei Schuld habe, deshalb habe er wissen wollen, wann er wieder arbeiten darf.

Daraus wurde bislang nichts: Porsche betonte bei der Beurlaubung zwar, man habe „keinerlei Hinweise" auf eine Mitverantwortung von Hatz für manipulierte Abgasmessungen. Dennoch kam Hatz im September 2017 in Untersuchungshaft. Erst im Juni 2018 kam er gegen eine Drei-Millionen-Kaution frei. Die Staatsanwaltschaft München II ermittelt wegen Betrugs-Verdachts gegen ihn. Die Ermittlungen wegen „Verletzung der Vertraulichkeit des Wortes" wurden dagegen eingestellt, weil, so eine Sprecherin, „keiner der Geschädigten Strafantrag gestellt hat". Die „Geschädigten", Porsche und Hatz' Anwalt Peter Gauweiler sagten zu den Protokollen nichts. Die Chancen auf Hatz' Rückkehr haben sich durch die Abhöraktion nicht erhöht (Mayr, Lauschangriff unter Kollegen, SZ 21.03.2019, 20).

Bayern

Polizei übt in Würzburg Ordnungs-Razzien nach neuem PAG

Die Hafentreppe am Heizkraftwerk in Würzburg ist ein Treffpunkt von Jugendlichen, die zumeist friedlich feiern. Da dort aber auch Minderjährige Alkohol konsumieren und es zu Körperverletzungs-, Raub- und Diebstahldelikten gekommen ist, führte die Polizei dort zwei drakonische Razzien mit umfassenden Erfassungsaktionen durch. Bei der Razzia am 22.03.2019 hielten 40 Einsatzkräfte 137 Jugendliche bis zu drei Stunden lang fest und durchsuchten sie. Bei der Razzia am 16.02.2019 wurden auch Fotos gemacht. Die Würzburger Polizeiaktionen wurden Gegenstand von Diskussionen im Bayerischen Landtag.

Ein 18-jähriger Schüler berichtet von dem Einsatz am 16.02.: „Wir wurden an die Wand gestellt, bekamen ein Schild mit einer Nummer in die Hand und wurden fotografiert. Ich war die Nummer 64." Auf Nachfrage stritt die Polizei zuerst ab, dass sie Personen abgelichtet hat, ohne dass es den Verdacht einer Straftat gab. Erst nachdem sich der 18-Jährige schriftlich beschwerte, gab die Behörde zu, man habe ihn und andere „ohne rechtliche Grundlagen" fotografiert. Gemäß Kathrin Thamm, Pressesprecherin des Polizeipräsidiums Unterfranken, sind neben den rechtlich nicht zulässigen Fotos bei der Aktion auch Aufnahmen mit einer Rechtsgrundlage gemacht worden: von Personen ohne Ausweis. Und von Verdächtigen einer vermeintlichen Sexualstraftat, bei der sich später herausgestellte, dass die „Berührungen und ungewollten Küsse" bereits eine Woche vorher passiert sein sollen. Am 11.03.2019 seien die Bilddateien gelöscht worden.

Bei der Großkontrolle am 22.03. waren hauptsächlich 14- bis 17-Jährige betroffen, die auf dem Weg zu einer Diskothek im Alten Hafen waren. Sie wurden auf Höhe des Cinemaxx-Kinos aufgegriffen, was nicht als gefährlicher Ort bezeichnet werden kann, und dann zur rund 200 Meter entfernten Hafentreppe gebracht. In einer Antwort auf eine Anfrage der Grünen-Fraktion erklärte Innenminister Joachim Herrmann (CSU) hierzu, die Einsatzkräfte hätten nicht feststellen können, wo die Jugendlichen vorher gewesen waren. Das Polizeipräsidium Unterfranken nannte dies später eine „Fehleinschätzung". Sprecherin Thamm sagte: „Dies bedauern wir ausdrücklich."

„Wir wurden aufgefordert, uns mit dem Gesicht an die Wand zu stellen", erzählte ein 17-Jähriger: „Nach drei Stunden Warten in der Kälte wurde ich zu einem Streifenwagen gebracht und musste meinen Personalausweis abgeben." Dann habe er seine Taschen ausleeren und einen Alkotest machen müssen und sei abgetastet worden. Drei weitere Schüler bestätigen diesen Ablauf. Auch alle anderen Anwesenden seien so durchsucht worden. Die Polizei erklärte, dass sie bei jeder Person Identität und Alter festgestellt habe, Durchsuchungen und Atem-Alkoholtests seien aber nur „anlassbezogen" erfolgt. Polizeisprecher Hein: „Bei 97 Personen wurden Atem-Alkoholisierungen festgestellt."

„Wir haben mehrmals gefragt, warum ich so lange festgehalten werde", berichtete ein Schüler. Eine Antwort habe er nicht bekommen. Bekommen haben er und alle seine Freunde am Ende einen Platzverweis. Laut Polizei sei dieser gegen alle „erkennbar betrunkenen Personen" ausgesprochen worden. „Das war ich sicher nicht" erklärte der Gymnasiast. Und ein 17-jähriger Betroffener fragte sich: „Darf die Polizei uns einfach so festhalten, uns durchsuchen, einen Alkotest machen und uns einen Platzverweis aussprechen, obwohl wir gar nichts gemacht haben?". Ein Betroffener berichtete ein Detail: „Als ich auf Toilette musste, wurde ich von Polizisten zum Rand der Treppe gebracht, um unter Aufsicht in den Main zu pinkeln." Das ist eigentlich eine Ordnungswidrigkeit, die laut städtischer Satzung mit einem Bußgeld belegt wird.

Das Ergebnis der Razzia, bei der neben den Einsatzkräften der Polizeiinspektion Würzburg eine geschlossene Einheit der Bereitschaftspolizei, ein Boot der Wasserschutzpolizei und ein Rauschgifthund im Einsatz waren, sind laut Polizei: drei Verstöße gegen das Betäubungsmittelgesetz und drei

alkoholisierte Minderjährige, die ihren Eltern übergeben wurden. Die vor Ort anwesenden Mitarbeiter des Kommunalen Ordnungsdienstes der Stadt Würzburg sollten Verstöße gegen das Stadtrecht ahnden. Doch passiert ist das laut Rathaussprecherin Claudia Lother nicht. Mitarbeiter des Jugendamtes haben sich darum gekümmert, dass unter 16-Jährige möglichst rasch den Platz verlassen konnten. Zu Details der Aktion wollte sich die Stadt aber nicht äußern: „Die Einsatzleitung oblag ja der Polizei." Bei der Polizeiinspektion Würzburg-Stadt hatten sich laut stellvertretenden Leiter Alexander Streng einige Eltern der betroffenen Jugendlichen gemeldet. Man habe diesen „die Notwendigkeit des Einsatzes nahe bringen" können.

„Jugendschutzkontrolle" nannte die Polizei zunächst den Einsatz. Auf Nachfrage ergänzte Polizeisprecher Steffen Hein: „Es hat Beschwerden von Anwohnern wegen Müll und Lärm auf der Hafentreppe gegeben." Im täglichen Polizeibericht, der an die Presse geht, wurde die Aktion dann nicht erwähnt. Bekannt wurde das polizeiliche Vorgehen erst durch Berichte von Betroffenen gegenüber der Presse. Klaus Böhm, Chef der Polizeiinspektion Würzburg, rechtfertigte den Einsatz: „Wir können doch nicht zusehen und warten, dass etwas passiert." Man habe durch die Großkontrollen Jugendliche vor Übergriffen sowie Drogen- und Alkoholmissbrauch schützen und Kriminalität verhindern wollen.

Rechtlich gedeckt sei der Einsatz, weil gemäß dem eben novellierten Bayerischen Polizeiaufgabengesetz (PAG) an „gefährlichen Orten", an denen Straftaten begangen werden, die Feststellung der Identität und Durchsuchungen prinzipiell erlaubt sei. Der Würzburger Strafverteidiger und Anwalt Markus Schüll sieht hier das gesetzliche Einfallstor: „Wenn die Polizei nachweisen kann, dass an der Hafentreppe regelmäßig Straftaten vorkommen und weitere zu erwarten sind, war die Maßnahme gerechtfertigt." Allerdings müsse die Einschränkung von Grundrechten wasserdicht begründet werden. „Wie die Polizei diese Rechtsgrundlage hier nutzt, könnte sie es prinzipiell auch auf einem Bierzelt oder bei einem Weinfest für eine ähnliche Aktion tun." Zum konkreten Vorgehen meinte er: „Ich kann nicht erst eine Person an einen gefährlichen Ort bringen, um die polizeiliche Maßnahme dann damit zu rechtfertigen, dass sich diese Person an einem gefährlichen Ort aufgehalten hat."

Der innenpolitische Sprecher der SPD-Fraktion, Stefan Schuster, fragte im Landtag an, ob die Polizei bei der „Jugendschutzkontrolle" Befugnisse aus dem neuen Polizeiaufgabengesetz nutzte. Man wolle wissen, ob die Jugendlichen auf der Hafentreppe aufgrund einer von ihnen ausgehenden „drohenden Gefahr" festgehalten und durchsucht wurden. Innenminister Herrmann erklärte in seiner Antwort, dass „drohende Gefahr" bei dem konkreten Fall keine Rolle gespielt habe. „Die Kontrollen wären vor der Änderung des Polizeiaufgabengesetzes möglich gewesen." Er verwies auf Ordnungs- und Sicherheitsstörungen, die in den vergangenen Wochen am Hafen vorgekommen seien. Dem gegenüber verwies die Würzburger Polizei als Rechtsgrundlage auf den neuen Art. 21 Abs. 1 Nrn. 1, 3 PAG, der eine Durchsuchung aufgrund einer „drohenden Gefahr für ein bedeutendes Rechtsgut" legitimiert.

Für den Datenschutzexperten Thilo Weichert steht das Würzburger Beispiel für „die Kultur der Bayerischen Polizei zu kontrollieren, Daten zu erfassen und zu speichern und dann zu schauen, wofür man sie brauchen kann". Der Politologe und Jurist aus Kiel ist ein Kritiker des neuen PAG: „Mit diesem hat die CSU-Politik der Polizei signalisiert, dass sie von rechtlichen Eingrenzungen frei gestellt werden soll." Würzburgs Polizeichef Böhm erklärte im Nachgang der öffentlichen Auseinandersetzung zu der Polizeiaktion, eine Nachbearbeitung sei „wichtig, um festzustellen, wo Fehler gemacht wurden". Nach den beiden Großkontrollen – den ersten dieser Art in Würzburg – räumte er ein: „So würden wir es nicht mehr machen." Im Alten Hafen sollen jetzt neben der Polizei auch verstärkt Sozialarbeiter tätig sein (Göbel, Hafen-Razzia: Polizei fotografierte Jugendliche, Mainpost 15.04.2019; Mainpost 05.04.2019; Mainpost 26.03.2019).

Bayern

ADG-Apothekensoftware speichert mehr Daten als nötig

Eine Apothekerin, die die Apothekensoftware der zur Phoenix-Group gehörenden Firma ADG, einem der größten Hersteller hierfür in Deutschland, nutzt, stellte fest, dass die Daten von KundInnen, die mit einem Rezept in ihre Apotheke kommen, ohne ihr Wissen gespeichert bleiben. Sie vermutet, dass viele Apotheken im Land das gleiche Problem haben ohne dies zu wissen. Die Vorwürfe werden vom zuständigen Bayerischen Landesamt für Datenschutzaufsicht LDA Bayern geprüft.

Die Apothekerin konnte nach einem halben Jahr noch immer nachsehen, welcher Kunde wann eine bestimmte Creme gekauft hat. Sie musste auf ihrem Computer nur den Namen eines Medikaments eingeben und schon listete der Rechner alle Verkäufe der vergangenen Monate auf, mit Vorname, Nachname, Anschrift, Geburtsdatum und Krankenkasse. In einer Zeile stand dann zum Beispiel „Text: Hans Meier". Das Wort „Text" ist der Hinweis darauf, dass Hans Meier kein Kundenkonto hat, sondern sich die Kasse den Namen vom Rezept gespeichert hat und Hans Meier davon wohl keine Ahnung hat.

Als sich die Apothekerin im Frühjahr 2018 um die Einhaltung der neuen Datenschutz-Grundverordnung (DSGVO) kümmern wollte und ihre Kundenkonten durchging, fiel ihr auf, dass mit der Software etwas nicht stimmen könne und dass sie viel mehr speichert als erlaubt ist. In ihrer Datei fand sie etwa 8650 KundInnen, ungefähr das Vierfache ihrer StammkundInnen, und fragte sich, zu wem all die anderen Konten gehören: „Ich habe mich mit meinem Mitarbeiter kurz ins System reingehängt. Es war erschreckend einfach."

Dominik Herrmann, Professor aus Bamberg, forscht und lehrt zum Datenschutz und zu Informationssicherheit. Er untersuchte die Software und fand schnell im unverschlüsselten Apothekennetzwerk das passende Passwort sowie massenhaft Kundendaten, die eigentlich gelöscht sein sollten. Der

Softwarehersteller ADG wies alle Schuld von sich: „Selbstverständlich können nicht (mehr) benötigte Daten auch von der Apotheke gelöscht werden, wobei jedoch ein abgestuftes Löschkonzept zum Tragen kommt.“ Es bestünden „zahlreiche gesetzliche Dokumentations- und Aufbewahrungspflichten für Apotheken“, etwa aus dem Steuerrecht, der Arzneimittelsicherheit oder dem Betäubungsmittelgesetz. Nach Ablauf der gesetzlichen Aufbewahrungsfristen würden die personenbezogenen Daten jedoch „irreversibel durch anonyme Daten überschrieben“. Auch bei der Prüfung desselben Systems bei einer weiteren Apotheke stieß Herrmann auf mehrere, ähnlich fragwürdige Vorgänge. Es gebe zwei Wege, um Kunden zu „löschen“. In Variante eins verschwinden die KundInnen aus der Anzeige, doch kann man sie mit einem Klick wieder zurückholen. In der zweiten, vermeintlich DSGVO-konformen Variante lassen sich die KundInnen nicht reaktivieren. In der Datenbank bleiben sie aber trotzdem gespeichert.

Als die Apothekerin das Geschäft von einer Vorgängerin übernahm, fragte diese bei ihren KundInnen nach, ob sie StammkundInnen bleiben wollen. Nur ein kleiner Teil stimmte zu. Die Firma ADG wurde daraufhin beauftragt, die Datenbank entsprechend zu bereinigen. Herrmann dazu: „ADG hätte die Aufgabe gehabt, die Datenbank ordentlich neu aufzusetzen. Das wäre aber ein erheblicher Programmieraufwand gewesen, um den man sich gedrückt hat“. Etwa 7.000 versteckte KundInnen ihrer Vorgängerin blieben so erhalten, entgegen rechtlicher Bestimmungen. Die ADG-Software erfasst auch Daten von KundInnen, die nur einmal vorbeikommen. Wird das Rezept beim Besuch der Apotheke eingescannt, passiert das mit einer Kamera, die den Text automatisch verarbeitet. In der Apotheke muss so die Adresse dann nicht mehr mit der Hand für die Abrechnung eingetippt werden, doch bleiben die Informationen auch nach der Abrechnung gespeichert.

Die Kamera erfasst unter anderem die Pharmazentralnummer, die jedem Medikament zugeordnet ist, Vorname, Nachname, Anschrift, Geburtsdatum und Krankenkasse. Grundsätzlich müssen Apotheker solche Daten von KassenpatientInnen erfassen, um die Medikamente abrechnen zu können. Die Apotheker scannen die Rechnungen separat ein und schicken sie an ein Apotheken-Rechenzentrum. Dazu müssen die Informationen aber nicht in einer Datenbank gespeichert bleiben; solange die KundInnen nicht zustimmen, dürfen sie das auch nicht. Die ADG-Software speichert die Daten offenbar trotzdem ab. Gemäß Bernhard Witt, Experte für Datenschutz und Informationssicherheit, steht diese Praxis in Konflikt mit dem Prinzip der Datenminimierung der DSGVO, wonach so wenig wie nötig gespeichert werden soll. Dies gelte erst recht, wenn PrivatpatientInnen ihre Rezepte nur vorlegen und selbst bezahlen.

Das eingeschaltete LDA Bayern beteuerte, dass das Thema „sehr hoch aufgehängt“ werde. Das Amt könne einen datenschutzkonformen Zustand der Software erzwingen, im Zweifel auch Bußgelder verhängen. Die ADG wehrte sich mit der Behauptung, dass die Warenwirtschaftssysteme den Anforderungen der DSGVO in vollem Umfang Rechnung tragen: „Datenschutz ist uns als Gesundheitsdienstleister sehr wichtig und durch Richtlinien und Prozesse fest in unserer Organisation verankert. Warenwirtschaftssysteme in Apotheken müssen den Anforderungen zahlreicher gesetzlicher Dokumentations- und Aufbewahrungspflichten für Apotheken genügen, die etwa aus dem Steuerrecht, dem BtM-Recht, der Arzneimittelsicherheit (zum Beispiel Arzneimittelrückrufe) oder den arzneimittelrechtlichen Sorgfaltspflichten des Apothekers zum Schutz von Patienten herrühren. Daher kommt ein abgestuftes, parametrisierbares Speicherungs- und Löschkonzept zum Tragen. Dieses Datenschutzkonzept ist für den Anwender umfassend dokumentiert, damit er die notwendigen Entscheidungen treffen kann.“

Auf die Frage, ob also die jeweilige Apotheke sich selbst um einen korrekten Datenumgang kümmern müsse, antwortete ein Sprecher des Unternehmens, das System S300 trage dem Grundsatz „privacy by default“ Rechnung, da es in den Standardeinstellungen auf maximalen Datenschutz eingestellt sei. Im datenschutzrechtlichen Sinne verantwortlich für die Datenerhebung und -verarbeitung sei aber die Apotheke. Sie könne in den Einstellungen des Systems jederzeit selbst bestimmen und einstellen, welche Daten erfasst und wie diese verarbeitet werden sollen. Dies sei in den Handbüchern zum Warenwirtschaftssystem auch klar beschrieben. So sei einstellbar, ob die Daten aus einem Rezept überhaupt übernommen werden sollen. Bei Rezeptscans könne man zudem eine konkrete Speicherdauer einstellen. Selbstverständlich könnten nicht (mehr) benötigte Daten auch von der Apotheke gelöscht werden, wobei jedoch ein abgestuftes Löschkonzept zum Tragen komme. Weiter erklärte er, dass es wichtig zu erwähnen sei, dass Aufbewahrungs- und Speicherfristen aus den unterschiedlichsten Gesetzen resultieren, etwa aus dem Handels-, Gewerbe-, Steuer-, Sozialrecht sowie Vorschriften des Gesundheitswesens. Bestünden gesetzliche Aufbewahrungspflichten, so gingen diese zwingend dem Grundsatz der Datenminimierung vor. Eine Löschung dürfe dann nicht erfolgen und könnte – wie etwa im Fall des Steuerrechts – sogar eine Straftat darstellen (Munzinger/Ratzesberger/Tanriverdi, Datenschutz Verdacht auf unzulässig gespeicherte Kundendaten in Apotheken, www.sueddeutsche.de 20.12.2018; Borsch, ADG widerspricht Datenschutzvorwürfen, www.deutsche-apotheker-zeitung.de 21.12.2018).

Berlin/Hessen

„Bild“ verweigert Staatsanwaltschaft Webnutzungsdaten

Am 25.03.2019 meldete die Bild-Zeitung auf Seite eins: „Staatsanwaltschaft will ´Bild` ohne Durchsuchungsbefehl durchsuchen.“ In vier Absätzen wurde geschildert, dass am vorangegangenen Samstagnachmittag Polizisten versucht hätten, „Zugang bei ´Bild` zu bekommen“. Die Ermittler hätten Zugriffsdaten von LeserInnen beschlagnahmen wollen. Man habe sie direkt am Eingang abgewiesen, da sie ohne richterlichen Durchsuchungsbeschluss gekommen seien. Bild-Chefredakteur Julian Reichelt wurde damit zitiert, dass seine Zeitung „wegen des hohen Gutes des unantastbaren Informantenschutzes

niemals freiwillig Daten von Lesern oder Informanten herausgeben" würde.

Auslöser war die Staatsanwaltschaft in Frankfurt am Main. Es handele sich um Ermittlungen des Landeskriminalamtes (LKA) von erheblicher Bedeutung wegen des Verdachts der Bedrohung und der Volksverhetzung in einem öffentlich bekannten Fall: Seit Dezember 2018 sucht die Staatsanwaltschaft nach den VerfasserInnen von üblen Drohungen und Beleidigungen gegen eine türkischstämmige Rechtsanwältin, welche die Familie eines NSU-Mordopfers vertreten hatte. Die TäterInnen hatten der Anwältin Drohbriefe gesandt und diese Drohungen mit „NSU 2.0" unterschrieben. In diesem Fall wird auch gegen mehrere inzwischen suspendierte Frankfurter Polizisten ermittelt, weil interne Daten aus dem Polizeicomputer in den Drohbriefen aufgetaucht sind (DANA 1/2019, 38 f.).

Kurz vor dem Besuch bei „Bild" waren die Ermittler offenbar auf Anhaltspunkte gestoßen, dass die Daten von Nutzenden der Webseite „bild.de" für ihre Ermittlungen relevant sein könnten. Die Frankfurter Staatsanwaltschaft meinte, dass „die Erhebung von Daten im Zusammenhang mit Zugriffen auf bestimmte, öffentlich zugängliche Online-Inhalte beim Axel-Springer-Verlag erforderlich" sei. Weil diese Nutzungsdaten nur für eine kurze Zeit gespeichert würden, habe die Staatsanwaltschaft den Axel-Springer-Verlag mittels Eilanordnung telefonisch und per Fax zur Herausgabe der Daten verpflichten wollen. Weil der Verlag nicht reagiert habe, sei dann an dessen Sitz in Berlin das dortige Landeskriminalamt um Unterstützung gebeten worden. Eine „Durchsuchung" der Geschäftsräume des Verlags sei zu keinem Zeitpunkt beabsichtigt gewesen. Es handele sich bei der Aktion nicht um einen Eingriff in die vom Grundgesetz geschützte Pressefreiheit, sondern um „das Anliegen, die im Raum stehenden massiven Straftaten mit zeugenschaftlicher Unterstützung durch ein Medienunternehmen aufzuklären".

Ein Sprecher des Axel-Springer-Verlags sieht dies anders: „Die Etikettierung der Vorgehensweise spielt für unseren Rechtsstandpunkt keine Rolle. Faktisch wollte das LKA Wiesbaden die Herausgabe von Leserdaten." Es sei ein legitimes Anliegen des Verlags, diese zu schützen. „Entscheidend ist, dass eine solche Herausgabeforderung unsere grundrechtlich geschützten Rechte berührt." Relevanz hätte allenfalls eine richterliche Anordnung und auch gegen diese würde die Redaktion, wie medial angekündigt, sämtliche Rechtsmittel ausschöpfen (Schneider, Nicht leicht zu haben, SZ 27.03.2019, 31).

Brandenburg

Fall Rebecca: Kfz-Kennzeichen-Vorratsdatenspeicherung

Die Polizei Brandenburg speichert Kennzeichen aller Autos auf bestimmten Autobahnen. Die Daten werden nicht nur nach Verdächtigen gerastert, sondern auch auf Vorrat gespeichert: Am 06.03.2019 teilten die Polizei und die Staatsanwaltschaft von Berlin im Fall eines verschwundenen Mädchens mit, dass das vom Tatverdächtigen genutzte Fahrzeug „am Tag des Verschwindens Rebeccas von einer Verkehrsüberwachungsanlage auf der Bundesautobahn (BAB) 12 zwischen Berlin und Frankfurt/Oder, am Montag, den 18. Februar 2019, um 10.47 Uhr und am darauf folgenden Tag, Dienstag, den 19. Februar 2019, um 22.39 Uhr, festgestellt wurde". Schon 2012 gab es Berichte, dass in Brandenburg Kennzeichen-Scanner nicht nur nach vorher definierten Kennzeichen fahnden, sondern mit einen „Aufzeichnungsmodus" auch sämtliche Kennzeichen speichern können. 2013 wurden die Standorte von vier stationären Geräten auf der BAB 12 veröffentlicht, bei denen es sich um das Produkt „PoliScan Surveillance" der Wiesbadener Firma Vitronic gehandelt haben soll. Gemäß Presseberichten zeigte sich die Polizei Brandenburgs „stinksauer", dass nun ihre Kollegen in Berlin die Ermittlungserkenntnisse öffentlich bekannt gemacht hatten.

2008 hatte das Bundesverfassungsgericht (BVerfG) eine „automatisierte Erfassung von Kraftfahrzeugkennzeichen" nur unter strengen Auflagen erlaubt. Ende 2018 hat es dann die Regelungen von Bayern, Baden-Württemberg und Hessen für teilweise verfassungswidrig erklärt (s. u. S. 108). Eine Kennzeichenerfassung kann in Brandenburg entweder gemäß dem dortigen Polizeigesetz präventiv oder zur Strafverfolgung gemäß der Strafprozessordnung (u. a. §§ 111, 100h, 163e StPO) erfolgen. Je nach Rechtsgrundlage gelten unterschiedliche Aufbewahrungs- und Löschfristen.

Patrick Breyer, Spitzenkandidat der Piratenpartei bei der Europawahl, kommentierte den Vorgang wie folgt: „Den gesamten Fahrzeugverkehr auf einer Strecke auf Vorrat zu speichern halte ich für eine völlig unverhältnismäßige Strafverfolgungsmaßnahme. Ich rate Betroffenen, rechtlich dagegen vorzugehen, um diese Frage vor Gericht klären zu lassen. Deutschland darf sich nicht die Praxis etwa von Dänemark oder Großbritannien zu eigen machen, die Bewegungen jedes Autofahrers aufzuzeichnen und bis zu zwei Jahre lang zu speichern."

Eine Sprecherin der Polizei Brandenburg bestätigte, dass das Auto im Fall Rebecca vom Kennzeichenerfassungssystem KESY protokolliert wurde. Dieses System enthalte einen Fahndungsmodus, der nach definierten Kennzeichen sucht, und einen Aufzeichnungsmodus, der sämtliche Kennzeichen erhebt und speichert. Das Kennzeichen des verdächtigen Autos war zum Erhebungszeitraum nicht im System zur Fahndung ausgeschrieben. Aber ein Richterbeschluss in einem anderen Strafverfahren hatte die Aufzeichnung sämtlicher Kennzeichen erlaubt. Und weil diese Daten schon erhoben und gespeichert waren, konnten sie auch im Nachhinein abgefragt und an die Berliner Polizei übermittelt werden. Die Brandenburger Polizei Brandenburg sprach hier explizit von „Beifang".

Die Landesdatenschutzbeauftragte Brandenburg (LfD) prüfte seit 2015 das System und ging dabei davon aus, „dass die Kameras ständig Kennzeichen aufzeichnen und daher bestimmte Straßenabschnitte entgegen der Entscheidung des Bundesverfassungsgerichts flächendeckend erfasst werden." Sie hatte Mängel gerügt und „eine andere Rechtsmeinung als die Polizei" vertreten. Ein Sprecher der LfD erklärte im Nachgang zu der Berichterstattung über den konkreten Fall Rebecca, dass nach der Prüfung im Jahr 2015 die Polizei die „Verfahrensdokumentation" des Systems nachgeliefert habe: „Im Ergebnis ihrer Auswertung haben wir hinsichtlich der Umsetzung der erforderlichen technisch-organisatorischen Maßnahmen

– auch unter Berücksichtigung der vorangegangenen Vor-Ort-Prüfung – keine gravierenden Mängel festgestellt." Eilfahndungen würden nach 24 Stunden gelöscht. Bei richterlichen Anordnungen von Beobachtungen oder Observationen hänge die Speicherfrist von der jeweiligen Dauer der Anordnung ab.

Darüber hinaus dürften Strafverfolgungsbehörden erhobene Daten zum Zwecke künftiger Strafverfahren gemäß § 484 StPO speichern. Die speichernde Stelle prüfe nach festgesetzten Fristen, ob die Daten zu löschen sind (sog. Aussonderungsprüfung). Die Prüffristen ergeben sich regelmäßig aus § 489 Abs. 4 StPO. Werden Daten zum Zwecke künftiger Strafverfahren in Dateien der Polizei gespeichert, gälten für die weitere Verwendung die Vorgaben des Brandenburgischen Polizeigesetzes (§ 484 Abs. 4 StPO i. V. m. §§ 37 ff. BbgPolG).

Clemens Arzt, Rechtswissenschaftler und Hochschullehrer, kritisierte die Bewertung der Landesdatenschutzbeauftragten. Er sehe nicht, dass Kennzeichendaten zufällig erfasster BürgerInnen aus strafprozessualem Anlass über längere Zeit gespeichert werden dürften. Weder für die Datenhebung noch für die Datenspeicherung gebe es eine entsprechende Befugnis der Polizei in der Strafprozessordnung. Die Einrichtung einer Kontrollstelle erlaube keine automatisierte Kennzeichenkontrolle, die Regelungen zur Observation bezögen sich nur auf Beschuldigte und erlaubten Datenerhebungen im Einzelfall. Die Ausschreibung eines Kennzeichens zur Beobachtung sei etwas völlig anderes als die Datenerhebung mittels automatisierter Kennzeichenkontrolle (Meister, Kennzeichenerfassung: Brandenburg speichert Autofahrten auf Vorrat, netzpolitik.org 07.03.2019 mit Updates).

Mecklenburg-Vorpommern

Datenschutzbeauftragter kritisiert Polizeigesetzentwurf

In einer internen Stellungnahme des Landesdatenschutzbeauftragten des Landes Mecklenburg-Vorpommern (LfDI) wird der Gesetzentwurf der Landesregierung zum neuen Sicherheits- und Ordnungsgesetz (SOG) als teilweise verfassungs- und europarechtswidrig kritisiert. Der Entwurf werde den Anforderungen an klare, präzise Regelungen und gute Verständlichkeit nicht gerecht und werde es der Polizei kaum möglich machen, ihre Aufgaben fehlerfrei zu erfüllen. Ende Januar 2019 hatte das Kabinett den Gesetzesentwurf gebilligt, welcher der Polizei mehr Rechte und Ermittlungsmethoden zur Gefahrenabwehr verschaffen soll. Vor allem an der Onlinedurchsuchung und der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) wird Kritik geübt. Die Polizei erhielte damit das Recht, mit einer Software unbemerkt in Computer, Smartphones oder Tablets einzudringen sowie Daten und Kommunikation abzugreifen. Dabei wird die Verschlüsselung vieler Chatprogramme umgangen. Um an die Geräte zu gelangen, sollen die Ermittler gemäß dem Gesetzentwurf auch heimlich in Wohnungen eindringen dürfen. Ein Richter muss zustimmen.

Das Innenministerium will die Befugnisse ausweiten, weil Kriminalität zunehmend übers oder im Internet begangen werde. Onlinedurchsuchung und Quellen-TKÜ sind bisher schon zur Ermittlung nach Straftaten erlaubt. Nun sollen die BeamtInnen des Landes beides bereits zur Gefahrenabwehr nutzen dürfen, also bevor eine Straftat geschehen ist. Dem LfDI fehlt es an unabhängiger Kontrolle. Das Bundesverfassungsgericht hat zum BKA-Gesetz im Jahr 2016 entschieden, dass schwerwiegende Eingriffe, die tief in die Privatsphäre der Betroffenen eindringen, nur verhältnismäßig sind, wenn die Polizei effektiv und unabhängig kontrolliert wird. Die Landesregierung plane hingegen, dass ein polizeiinterner Beauftragter die Ermittler kontrollieren, das erlangte Material sichten und auf die Einhaltung der Regeln achten soll. Um die vom Verfassungsgericht aufgestellten Anforderungen zu erfüllen, müsse der LfDI die Polizei kontrollieren können. Dem fehlten jedoch Befugnisse, weil MV eine dafür nötige EU-Richtlinie noch nicht in Landesrecht überführt habe.

Aufmerksamkeit widmet die Stellungnahme des LfDI auch dem Kfz-Kennzeichen-Scannen. Das soll weiterhin von den Grenzen bis einschließlich der A20 erlaubt bleiben. Das Bundesverfassungsgericht hatte im Dezember 2018 das Kennzeichenscannen nur bis maximal 30 Kilometer von der Grenzen entfernt erlaubt und die Regelungen einiger Bundesländer für nichtig erklärt (s. u. S. 108). Wenn die Polizei Personen und ihre Sachen durchsucht, soll sie nach dem Entwurf auch auf Speichermedien und Cloud-Speicher zugreifen dürfen. Weil dies mitunter den Kernbereich der geschützten Privatsphäre betreffen kann, fordern die Datenschützer, dass ein Richter der Speicherdurchsuchung zustimmen muss.

Weitere Kritikpunkte betreffen zum Beispiel Videoaufnahmen der Polizei, etwa von Demonstrationen, mit Bodycams, Drohnen oder Kameras in Einsatzfahrzeugen. Die Videos sollen den Plänen zufolge auch unverpixelt als Schulungsmaterial für die Polizeiausbildung genutzt werden. Dies ist für die Datenschützer ein klarer Verstoß gegen europäisches Datenschutzrecht. Außerdem werden fehlende oder unvollständige Lösch- und Prüffristen für Daten bemängelt, was gegen europäisches Recht verstieße.

Grundsätzlich fordert der Datenschutzbeauftragte, bei Verstößen von Behörden auch gegen diese tätig werden zu dürfen. Zwar kann seine Behörde eine andere Behörde zum Beispiel anweisen, bestimmte Daten zu löschen. Durchsetzen kann er diese Anweisung aber nicht. Anders als gegen Firmen oder Privatleute darf der Datenschutzbeauftragte keine Zwangsgelder gegen öffentliche Stellen verhängen. Behörden müssten also nicht fürchten, bestraft zu werden, sollten sie Rechte von Betroffenen verletzen, bemängeln die Autoren der Stellungnahme. Das Innenministerium wollte sich zu den Kritikpunkten nicht näher äußern. Die Stellungnahmen zum Gesetzentwurf würden derzeit geprüft (Polizeigesetz Mecklenburg-Vorpommern: Kritik von Datenschutzbehörde, www.heise.de 17.03.2019, Kurzlink: https://heise.de/-4338494).

Niedersachsen

Polizei baut Fake-Radarfalle ab

AnwohnerInnen in Leeseringen/Kreis Nienburg haben eine täuschend echt aus-

sehende Blitzer-Attrappe gebaut und an die Straße gestellt, weil sie sich ständig über Temposünder auf der Bundesstraße 215 ärgerten. Eine Streifenwagen-Besatzung entdeckte die Anlage Mitte März 2019 zufällig beim Vorbeifahren. Neben einem Kasten der Marke Eigenbau hatten die AnwohnerInnen eine echte Kamera postiert, von der ein Kabel zu einem Wohnhaus führte. Ob mit dem Apparat tatsächlich Fotos von Temposündern gemacht oder möglicherweise bei Bedarf Blitzlichter ausgelöst wurden, wurde daraufhin von der Polizei überprüft. Diese fand die handwerkliche Ausführung des Self-Made-Blitzers beachtlich. Das hinderte sie aber nicht, ein Verfahren wegen Amtsanmaßung einzuleiten, was mit Geld- oder Freiheitsstrafe bis zu zwei Jahren geahndet werden kann. Der Polizeisprecher bestätigte, dass auf der B 215 im Kreis Nienburg vielerorts zu schnell gefahren wird, weshalb Polizei und Landkreis häufig mit mobilen Messanlagen unterwegs seien. Wohl aus Ärger darüber hatte ein Autofahrer in Nienburg eine solche Messanlage demoliert; diesen erwartet nun ein Strafverfahren.

Blitzer-Attrappen sorgen immer wieder für Aufsehen. So stellte eine Bürgerinitiative Dezember 2018 in Isernhagen in der Region Hannover eine täuschend echt wirkende Blitzersäule auf. Aus Sicht der Polizei ist gegen die Säule nichts einzuwenden, da sie auf einem Privatgrundstück steht. Anders erging es einem Tischler in Köln, der mit seinen Kindern ebenfalls eine Attrappe gebaut und aufgestellt hatte. Ein Gericht bewertete dieses Verhalten als strafbar. Auch außerhalb von Niedersachsen ist die Eigeninitiative beliebt. In einem kleinen Dorf bei Travemünde stellte ein durch Raser verärgerter Anwohner einen unechten „Starenkasten" auf seinem Grundstück auf (Ärger über Raser: Anwohner stellen Blitzer-Attrappe auf, www.goettinger-tageblatt.de 19.03.2019).

Rheinland-Pfalz

Weitergabe von Daten über Asylsuchende beanstandet

Die Kreisverwaltung Germersheim hat persönliche Daten von 15 Asylbewerbenden weitergegeben und dafür zwei Verwarnungen des Landesbeauftragten für Datenschutz Rheinland-Pfalz (LfD) kassiert. In beiden Fällen habe der Kreis eine andere Rechtsauffassung und klagte gegen den Tadel, sagte eine Behördensprecherin am Montag in Germersheim. Nach eigenen Angaben hatte die Kreisverwaltung eine zunächst anonyme Statistik der als gefährlich eingestuften Asylbewerber versehentlich mit Klarnamen an das zuständige Ministerium und an Abgeordnete gegeben. Obwohl die Behörde umgehend Schritte gegen die Verwendung der Informationen unternommen habe, wurde sie vom LfD gerüffelt.

Die zweite Kritik des Datenschutzbeauftragten betraf eine Umfrage der Kreisverwaltung bei Verbandsgemeinden. Anlass war die Anfrage einer Verbandsgemeindeverwaltung an den Landrat wegen eines mehrfach auffällig gewordenen Asylbewerbers. Der LfD beanstandete, dass bereits im ersten Schritt Namen abgefragt wurden, was nicht notwendig gewesen sei. Landrat Fritz Brechtel (CDU) erklärte: „Es liegt sowohl im Interesse der Sicherheit der Bürgerinnen und Bürger als auch im Interesse der Rechtsklarheit, diese unterschiedlichen Rechtsauffassungen klären zu lassen". Die Verwaltung sei für die Sicherheit der Menschen verantwortlich – dazu gehöre der Austausch von Daten (Streit um Datenschutz für Asylbewerber, www.wiesbadener-kurier.de, 3. Januarwoche 2019).

Sachsen

Polizeigesetz mit mehr Befugnissen verabschiedet

Der sächsische Landtag hat am 10.04.2019 die strittige Reform des Polizeigesetzes beschlossen, mit dem die Ordnungshüter des Freistaats viele neue Befugnisse erhalten. So wird die Videoüberwachung deutlich ausgeweitet – vor allem auf Verkehrsrouten, die für „grenzüberschreitende Kriminalität" zur Verschiebung von Diebesgut genutzt werden oder Tatorte des Menschenhandels sind. Die Polizei darf künftig innerhalb eines 30-Kilometer-Korridors entlang der Grenzen zu Polen und Tschechien versuchen, Schwerverbrecher mit Videoaufnahmen sowie automatischer Gesichtserkennungs-Software ausfindig zu machen.

Kommunen können künftig in Eigenregie Maßnahmen zur Videoüberwachung veranlassen. Scanner für den automatisierten Abgleich von Kfz-Kennzeichen sollen an sächsischen Straßen verstärkt eingesetzt werden. Polizisten sollen mit Bodycams ausgerüstet werden. Darauf hatten sich die Regierungsfraktionen von CDU und SPD zuvor geeinigt. Ein Kabinettsentwurf wurde entsprechend geändert. Den Ermittlern soll zudem eine „präventive Telekommunikationsüberwachung" sowie das Abbrechen von Mobilfunkverbindungen mithilfe von Störsendern erlaubt und der Einsatz von IMSI-Catchern zur Standortermittlung erleichtert werden.

Die Polizei darf zudem Daten bei Internetkonzernen wie Amazon, Facebook oder Google abfragen. Spezialeinheiten etwa zur Terrorabwehr sollen in besonderen Einsatzsituationen Waffen mit erforderlicher Reichweite und hoher Durchschlagskraft wie Maschinengewehre oder Handgranaten nutzen dürfen. Auch nicht-tödliche Munition darf verwendet werden. Elektronische Fußfesseln können Gefährdern angebracht werden, um Aufenthalts- oder Kontaktverbote zu überwachen. Generell soll die Polizei vermehrt schon „im Vorfeld einer konkreten Gefahr" eingreifen dürfen. Mehr Befugnisse zur Abwehr einer „dringenden Gefahr" sind vorgesehen, wenn „das Ausmaß des zu erwartenden Schadens und die Wahrscheinlichkeit des Schadenseintritts" besonders hoch sind.

Nicht durchsetzen konnte sich die CDU mit ihren Rufen nach Kompetenzen im polizeilichen Abwehrrecht für heimliche Online-Durchsuchungen und für den Einsatz von Staatstrojanern zur Quellen-Telekommunikationsüberwachung, die insbesondere auf Messenger-Dienste wie WhatsApp zielt. Der sächsische Datenschutzbeauftragte Andreas Schurig hatte vorab ebenso wie Bürgerrechtsorganisationen vor einem „hohen verfassungsrechtlichen Risiko" vor allem durch die unausgereifte, in ihren Folgen kaum abschätzbare und ethisch nicht vertretbare Gesichtserkennung gewarnt. Linke und Grüne lehnten die Reform als massiven „Schlag gegen die Bürgerrechte" ab, mit dem auch vermehrt Unverdächtige in die Überwachungsmaschinerie gerieten. Sie wollen beim Verfassungsgerichtshof Klage ein-

reichen. In Kraft treten sollen die neuen Bestimmungen Anfang 2020 (Krempl, Sachsen: Polizei darf Verbrechen mit Gesichtserkennung und Handgranate bekämpfen, www.heise.de 10.04.2019, Kurzlink: https://heise.de/-4374641).

Sachsen-Anhalt

Bußgeld gegen Behördentroll wegen nicht versteckten E-Mail-Empfängern

Der Landesdatenschutzbeauftragte von Sachsen-Anhalt, Harald von Bose, hat wegen Datenschutzverstößen durch offene E-Mail-Verteiler mehrere Geldbußen gegen einen „Behördentroll“ aus Merseburg festgesetzt. Dieser habe wiederholt Mails mit hunderten personenbezogenen E-Mail-Adressen im offenen Verteiler verschickt und die EmpfängerInnen nicht im BCC versteckt.

Bei den Mails handelte es sich demnach um Beschwerden, Stellungnahmen, Verunglimpfungen sowie um Strafanzeigen gegen Vertreter aus Wirtschaft, Presse, Kommunal- und Landespolitik. Fast täglich seien Mails verschickt worden, zum Teil an bis zu 1.600 Adressen. Zwar seien die Inhalte legitim, jedoch nicht der Umgang mit den Daten der EmpfängerInnen. Von Bose erläuterte: „Der Mann hat sich uns gegenüber immer wieder auf die Meinungsfreiheit berufen, aber diese gestattet keine solchen offenen Verteiler. Der Grund ist, dass dadurch ja Rechte Dritter berührt werden. Wir waren in dieser Sache sehr akribisch, haben jeden einzelnen Verstoß sehr genau aufgelistet, um das Ganze auch gerichtsfest zu machen, falls das nötig werden sollte.“

Die verschiedenen Bußgelder summierten sich auf 2.628,50 Euro. Die Mitteilung über die Geldbuße wurde am 05.02.2019 zugestellt, bereits tags drauf ging die Zahlung ein. Möglicherweise wird es weitere Verfahren geben, weil der Mann auch nach den Bußgeldbescheiden gegen den Datenschutz verstoßen haben soll. Gemäß Art. 2 Abs. 2 lit. c DSGVO findet die Datenschutz-Grundverordnung (DSGVO) keine Anwendung bei der Datenverarbeitung „durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“. Im privaten Umfeld wäre demgemäß ein offener E-Mail-Verteiler erlaubt. Für die hier praktizierte Kommunikation außerhalb dieses Bereichs galt diese Ausnahme jedoch nicht (Greis, Datenschutz: Hohes Bußgeld wegen offenen E-Mail-Verteilers, www.golem.de 14.02.2019).

Datenschutznachrichten aus dem Ausland

Weltweit

Quartalsbericht Facebook

Facebook rechnet damit, dass die jüngsten von ihm zu verantwortenden Datenschutz-Skandale das Plattform-Unternehmen bis zu 5 Mrd. Dollar kosten werden. Im Zusammenhang mit entsprechenden Ermittlungen der US-Handelsbehörde Federal Trade Commission (FTC) legte Facebook im ersten Quartal 2019 bereits 3 Mrd. Dollar für mögliche Strafzahlungen beiseite. Insgesamt könne die Belastung auch 5 Mrd. Dollar erreichen, erklärte das Unternehmen. Auslöser für die Untersuchung war vor allem der Skandal um Cambridge Analytica. Mit Geldreserven von über 45 Mrd. Dollar könnte das Unternehmen die erwarteten Strafzahlungen leicht verdauen. Die Anleger zeigten sich entspannt nach der Ankündigung im April 2019: Die Aktie legte im nachbörslichen Handel um mehr als 7% zu. Relevanter als der Geldbetrag könnten aber die Auflagen sein, die die FTC bei Facebook durchsetzen kann.

Die Rückstellung drückte den Gewinn im 1. Quartal 2019 auf 2,43 Mrd. Dollar nach knapp fünf Mrd. ein Jahr zuvor. Der Umsatz stieg im Jahresvergleich um 26% auf gut 15 Mrd. Dollar. Nach wie vor werden 93% der Werbeerlöse auf Mobilgeräten wie Smartphones erwirtschaftet. Die Zahl monatlich aktiver Facebook-Nutzender wuchs binnen drei Monaten um rund 60 Millionen auf 2,38 Mrd. Täglich griffen auf das Online-Netzwerk 1,56 Mrd. Nutzende zu – nach 1,52 Mrd. im Vorquartal.

Über alle Facebook-Angebote hinweg – einschließlich der Chatdienste WhatsApp und Messenger sowie der Foto-Plattform Instagram – waren 2,7 Mrd. Nutzende aktiv, davon 2,1 Mrd. täglich. Die Zuwächse stammten vor allem aus Asien. In Europa legte die Zahl der mindestens einmal im Monat aktiven Nutzenden um drei Millionen auf 384 Mio. zu. Im Jahr 2018 war die europäische Nutzerzahl zeitweise zurückgegangen. Grund dafür war vermutlich die Umstellung durch die Datenschutz-Grundverordnung DSGVO, bei der neue Zustimmungen zur Datenverarbeitung eingeholt werden mussten.

Die Zahl der Beschäftigten wuchs seit Jahresbeginn 2019 von knapp 35.600 auf fast 37.800. Facebook erweitert unter anderem ständig die Teams, die unerlaubte oder kriminelle Inhalte löschen. Das Online-Netzwerk stand im vergangenen Quartal unter anderem in der Kritik, weil das Live-Video des verheerenden Anschlags auf zwei Moscheen im neuseeländischen Christchurch über die Facebook-Plattform gestreamt worden war. Facebook-Chef Mark Zuckerberg bekräftigte, dass er das Online-Netzwerk stärker auf verschlüsselte Kommunikation in Chat-Diensten ausrichten wolle und das noch unklare Auswirkungen auf das Geschäftsmodell haben werde. Die Umstellung sei aber ein langer Prozess (Facebook legt Mrd. für Strafzahlung beiseite, www.morgenweb.de 26.04.2019).

Weltweit

Amazon analysiert Alexa-Sprachinhalte

Durch die Analyse von aufgenommenen Sprachbefehlen will Amazon seinen Sprachassistenten Alexa verbessern und nimmt dafür Zugriff auf die privaten Inhalte der Nutzenden. Dies wurde von dem Konzern bestätigt: „Wir versehen nur eine sehr geringe Auswahl an Alexa-Sprachaufnahmen mit Kommentaren, um das Kundenerlebnis zu verbessern.“

Gemäß Presseberichten wird dies an mehreren Standorten weltweit erledigt, unter anderem in Boston, Costa Rica, Indien und Rumänien. Laut zwei Mitarbeitenden in Bukarest schlagen sie dort pro Schicht bis zu 1.000 Mitschnitte um. Ein Mitarbeiter aus Boston sagte, er habe zum Beispiel Aufzeichnungen mit den Worten „Taylor Swift“ analysiert und sie mit der Anmerkung versehen, dass die Nutzenden die Sängerin meinten.

Hin und wieder bekämen sie so aber auch Zugang zu privaten Inhalten oder würden sogar Zeugen von möglicherweise kriminellen Vorgängen. Zwei Mitarbeiter berichteten von einem Mitschnitt, den sie als sexuellen Übergriff deuteten. Zwei Mitarbeitenden des Standorts Bukarest zufolge gilt bei Amazon in solchen Fällen die Auffassung, es sei nicht die Aufgabe des Unternehmens, einzuschreiten. Laut Aussage von Mitarbeitenden werden teilweise auch sehr private Audionachrichten in größeren Team-Meetings besprochen. In internen Chat-Kanälen würden amüsante Audioclips geteilt. Sie wiesen darauf hin, dass in vielen Aufzeichnungen das Schlüsselwort, meistens „Alexa“, fehlte – gemäß einem Mitarbeiter bei etwa 10% der Audioclips.

Amazon betonte, man achte bei dem Verfahren auf den Schutz der Privatsphäre der Nutzenden. „Beschäftigte haben keinen direkten Zugang zu Informationen, durch die eine Person oder ein Account bei diesem Verfahren identifiziert werden können“. Gemäß der Berichte waren jedoch auf einem Screenshot zu einem Transkriptionsauftrag eine Accountnummer, der Vorname des Nutzers sowie die Seriennummer des Geräts aufgeführt gewesen. Der Konzern erklärte, alle Informationen würden streng vertraulich behandelt und es werde mit Zugangseinschränkungen und Verschlüsselung gearbeitet. Bei Missbrauch des Systems gelte eine „Null-Toleranz-Regel“. Dass Mitarbeitende die Audionachrichten abhören, diene dazu, die Qualität der Antworten zu verbessern. Das gelinge, indem die menschlichen HelferInnen die automatischen Transkriptionen, die Sprachassistenten von den Anfragen anfertigen, korrigieren und die verbesserte Antwort an die künstliche Intelligenz zurückschicken. Im besten Fall kann bei der nächsten ähnlichen Anfrage ein besseres Ergebnis ausgeworfen werden.

Die Konkurrenten Apple und Google äußerten sich nicht zur Anfrage, ob sie auf eine ähnliche Vorgehensweise bei ihren Assistenten Siri und Google Assistant zurückgreifen.

Anne Spiegel (Grüne), rheinland-pfälzische Verbraucherschutzministerin und Vorsitzende der Verbraucherschutzministerkonferenz, forderte nach Bekanntwerden der Praxis Amazon auf, das Abhören von BürgerInnen sofort zu stoppen. Zudem müssten die Aufsichtsbehörden für den Datenschutz die Nutzungsbedingungen von Amazon dringend überprüfen: „Das Abhören persönlicher Gespräche in der eigenen Wohnung ist ein extremer Eingriff in die Persönlichkeitsrechte. Die Betroffenen müssen unverzüglich informiert werden.“ Aus Amazons Nutzungsbedingungen gehe nicht eindeutig hervor, dass die Kommunikation mit dem Sprachassistenten nachträglich von Mitarbeitenden angehört und schriftlich festgehalten werden könne.

Die Nutzungsbedingungen für Alexa geben tatsächlich keine konkreten Hinweise auf diese Praxis. Es heißt nur, Alexa verarbeite die Anfragen der Nutzenden „in der Cloud“. In den Privatsphäre-Einstellungen des Sprachassistenten haben Nutzende die Möglichkeit, der Verwendung ihrer Daten zur Weiterentwicklung des Systems zu widersprechen. Aus den Informationen geht bisher allerdings nicht explizit hervor, dass unter Umständen auch Menschen die Aufzeichnungen des Geräts anhören könnten. Wer nicht möchte, dass Amazon möglicherweise ihre Fragen an den Sprachassistenten abhört, sollte so vorgehen: „In den zugehörigen Apps der Sprachassistenten für iOS und Android kann man links oben auf das Menü-Symbol klicken, meistens als drei kleine Streifen zu erkennen. Unter Einstellungen/Alexa-Konto/Alexa Datenschutz findet man ganz unten die Option ´Legen Sie fest, wie Ihre Daten Alexa verbessern sollen.` “ Die beiden angebotenen Optionen sollten dann deaktiviert werden. Doch will Amazon die KundInnen davon abhalten: Diese werden gewarnt, dass neue Funktionen bei ausgeschalteter Option „möglicherweise nicht ordnungsgemäß“ arbeiten (Muth, Amazon hört zu, wenn jemand unter der Dusche Tylor Swift singt, SZ 12.04.2019, 26; Sprachassistent Amazon wertet Alexa-Aufnahmen aus, www.tagesschau.de 13.04.2019; Verbraucherschutzministerin fordert Stopp des Abhörens über Alexa, www.heise.de 13.04.2019).

EU

DSGVO: Viele Beschwerden, bisher wenig Sanktionen

Im Vorfeld des Datenschutztages 2019 teilte die EU-Kommission mit, dass seit Inkrafttreten der EU-Datenschutzgrundverordnung (DSGVO) bis Januar 2019 die Datenschutzbehörden der EU-Staaten mehr als 95.000 Beschwerden von BürgerInnen erhalten haben. Sie berichtete über drei Strafen gegen Unternehmen nach der seit Mai 2018 geltenden DSGVO: In Frankreich wurde Google wegen fehlender Zustimmung zu Werbung zu 50 Millionen Euro verurteilt, in Deutschland ein sozialer Netzwerkbetreiber zu 20.000 Euro wegen fehlender Sicherung von Benutzerdaten, und in Österreich ein Wettcafé wegen illegaler Videoüberwachung zu 5.280 Euro. Die Leiterin der österreichischen Datenschutzbehörde und Vorsitzende des Europäischen Datenschutzausschusses, Andrea Jelinek, bestätigte den österreichischen Fall. Der Entscheid sei noch nicht rechtskräftig, es laufe eine Anfechtung vor dem Bundesverwaltungsgericht. Das betroffene Unternehmen werde anonym gehalten. Es sei aber „kein großer Player“, sagte Jelinek (zu Portugal siehe DANA 4/2018, 210; zu Deutschland s. o. S. 88).

EU-Kommissions-Vizepräsident Frans Timmermans erklärte: „Wir sind stolz, die strengsten und modernsten Datenschutzbestimmungen weltweit zu haben, die zum globalen Standard werden.“ Der Skandal um Facebook und Cambridge Analytica (DANA 4/2018, 210) und jüngste Verstöße würden zeigen, dass die EU den richtigen Weg gehe. „Es steht nicht nur der Schutz unserer Privatsphäre auf dem Spiel, sondern auch der Schutz unserer Demokratien und die Nachhaltigkeit unserer von Daten betriebenen Wirtschaft.“ Die EU-Kommission verwies auch auf jüngste

Datenschutzabkommen mit Japan (s. u. S. 100). Fünf EU-Staaten haben gemäß Kommissionsangaben die Verordnung noch nicht vollständig in nationales Recht umgesetzt. Sie rief Bulgarien, Griechenland, Slowenien, Portugal und Tschechien dazu auf, dies so rasch wie möglich zu tun (Bisher schon 95.000 Datenschutz-Beschwerden eingelangt, www.tt.com 26.01.2019).

EU

Einigung über Whistleblower-Schutz

In der Nacht des 12.03.2019 haben sich Unterhändler der EU-Staaten, des Europäischen Parlaments (EP) und der EU-Kommission auf eine Richtlinie zum Schutz von Hinweisgebern geeinigt. Künftig sollen etwa ArbeitnehmerInnen, die Verstöße in ihrem Unternehmen oder ihrer Organisationen offenlegen wollen, keine Repressalien mehr zu befürchten haben. Nach dem Willen der EU-VerhandlerInnen soll niemand mehr aus Angst vor Vergeltung abgehalten werden, seine Bedenken zu äußern. Den Vorschlag zur Richtlinie machte die EU-Kommission im April 2018. Im November positionierte sich das Parlament auf Vorschlag von Berichterstatterin Virginie Rozière von den französischen Sozialisten für einen deutlich stärkeren Schutz als ursprünglich von der Kommission vorgeschlagen. Die EU-Staaten blockierten zunächst eine Einigung.

So hatten sich das deutsche Bundesjustizministerium von SPD-Politikerin Katarina Barley und weitere Stimmen im Rat für ein dreistufiges Verfahren ausgesprochen. Danach hätten Whistleblower sich immer zuerst an eine interne Stelle in der eigenen Organisation wenden müssen und dann an eine Aufsichtsbehörde außerhalb, bevor sie Informationen nach außen weitergeben dürfen. Das Europaparlament hatte hingegen darauf gedrungen, dass WhistleblowerInnen selbst wählen können, wie und wo sie Alarm schlagen. Die erzielte Einigung hält im Prinzip zwar an dem dreistufigen Meldeverfahren fest. Der Weg über betriebsinterne Kanäle ist laut EU-Kommission aber nur vorgeschrieben, wenn das Problem so auch tatsächlich „wirksam angegangen“ werden kann und die Hinweisgeber „keine Vergeltungsmaßnahmen riskieren“. Andernfalls könnten sie sich an die Behörden wenden. In bestimmten Fällen dürfen Whistleblower auch an die Öffentlichkeit gehen, etwa über Medien. Dies wird z. B. erlaubt, wenn Behörden nicht angemessen auf einen gemeldeten Missstand reagieren, das öffentliche Interesse gefährdet oder das Melden an die Behörde aus gewichtigen Gründen keine Option ist. Letzteres könne der Fall sein, wenn die betroffene Behörde und der Straftäter Absprachen getroffen haben.

Ohne Whistleblowing wären Enthüllungen wie die Lux Leaks oder die Panama Papers wohl nie an die Öffentlichkeit gelangt. Mit ihren Hinweisen deckten die InformantInnen Missstände auf und stießen eine weltweite Debatte über Steuergerechtigkeit an. EU-Kommissionsvizepräsident Frans Timmermans: „Whistleblower tun das Richtige für die Gesellschaft und sollten von uns geschützt werden, damit sie dafür nicht bestraft, entlassen, degradiert oder vor Gericht verklagt werden.“ EP-Abgeordnete begrüßten die Einigung. Die Länder, die eine Einigung blockiert hätten, seien von der Zivilgesellschaft und NGOs zu einer Lösung bewegt worden, so deren Chefverhandlerin Rozière.

Die Nichtregierungsorganisation Transparency International bezeichnete das Verhandlungsergebnis als „historisch“. Der Deutsche Gewerkschaftsbund reagierte ebenso positiv: „Eine solche Regelung macht es wahrscheinlicher, dass Wirtschaftsskandale mit Hilfe von integren und mutigen Beschäftigten ans Licht kommen und diese gleichzeitig vollen Schutz genießen.“ Anwendungsfälle für die neue Regelung werden voraussichtlich Verstöße gegen EU-Recht bei Geldwäsche, Unternehmensbesteuerung, Daten- und Umweltschutz sowie Lebensmittelsicherheit sein. Die EU-Staaten und das Europäische Parlament müssen die Einigung noch formell bestätigen. Anschließend müssen die Mitgliedsländer die neuen Regeln in nationales Recht umwandeln. EU-Justizkommissarin Věra Jourová sprach von einem „ausgewogenem System“. Arbeitgeber würden ermutigt, Probleme intern zu lösen. Hinweisgeber hätten auch andere Möglichkeiten – „ohne Angst vor Vergeltung haben zu müssen“. Der grüne Europaabgeordnete Sven Giegold ergänzte: „Whistleblower bekommen in Europa künftig den Schutz, den sie verdienen“ (Mühlauer, Recht zum Alarm schlagen, SZ 13.03.2019, 18; Fanta, EU-Verhandler einigen sich auf mehr Schutz für Whistleblower, netzpolitik.org 13.03.2019; zum Schutz von Whistleblowern nach deutschem Recht s. o. S. 86).

EU

EDPS überprüft behördliche Microsoft-Nutzung

Der Europäische Datenschutzbeauftragte (European Data Protection Supervisor – EU-Datenschutzbehörde EDPS) untersucht gemäß einer Mitteilung vom 08.04.2019, ob die Verträge der EU-Dienststellen mit Microsoft der seit Ende 2018 geltenden Datenschutzgrundverordnung (DSGVO) entsprechen. Die Institutionen der EU nutzen Microsofts Produkte und Dienstleistungen für die alltägliche Arbeit. Dabei werden große Mengen an persönlichen Daten verarbeitet. Der EDPS will zunächst erfassen, welche Produkte und Dienstleistungen von Microsoft bei der EU im Einsatz sind. Dann will die Datenschutzbehörde feststellen, ob die zugrundeliegenden vertraglichen Regelungen den Anforderungen der DSGVO entsprechen.

Mit der DSGVO sind Dienstleister selbst für den Datenschutz verantwortlich. Der stellvertretende EU-Datenschutzbeauftragte Wojciech Wiewiórowski erläuterte: „Allerdings bleiben die EU-Institutionen für Datenverarbeitungen in ihrem Namen verantwortlich, wenn sie auf Dienstleister zurückgreifen. Sie sind darüber hinaus verpflichtet sicherzustellen, dass die vertraglichen Abmachungen den Regeln entsprechen.“

Der EDPS verweist auf eine im November 2018 veröffentlichte Untersuchung des niederländischen Justizministeriums, die beim Einsatz der Enterprise-Version von Microsoft Office in Behörden zahlreiche Verstöße gegen die DSGVO festgestellt hatte. Ein Befund war demnach, dass Microsoft Office „systematisch Daten in großem Umfang“ erfasse,

„ohne die Nutzer darüber zu informieren“. Auch hätten die Nutzenden keine Kontrolle über Art und Umfang der Datennutzung (Briegleb, DSGVO: Datenschützer untersucht EU-Verträge mit Microsoft, www.heise.de 09.04.2019, Kurzlink: https://heise.de/-4367881).

EU

Trilog: der EU-Ausweis mit obligatorischen Fingerabdrücken

Die Verhandlungsführenden des EU-Parlaments, des Ministerrats und der EU-Kommission haben sich am 19.02.2019 im Trilog auf eine neue Verordnung für sicherere Dokumente für den Identitätsnachweis geeinigt. Darin wird künftig vorgeschrieben, dass zwei digitale Fingerabdrücke in neu ausgestellten Ausweispapieren enthalten sind. Zugriff auf die erweiterten biometrischen Daten sollen insbesondere Polizei, Zoll, Steuerfahndung und Meldebehörden erhalten. Bisher sind Fingerabdrücke nur im Reisepass verpflichtend. Die EU-Kommission hat schon im April 2018 eine „Verordnung zur Verbesserung der Sicherheit von Personalausweisen und Aufenthaltstiteln für EU-Bürger und ihre Familienangehörigen“ vorgeschlagen. Darin werden verschiedene Maßnahmen vorgeschlagen, um die in der EU kursierenden Personalausweise zu vereinheitlichen.

Bisher sind die Ausweise der EuropäerInnen ziemlich unterschiedlich. Untersuchungen zufolge sind in den Mitgliedstaaten der Union bisher mindestens 86 verschiedene Personalausweise mit oftmals unterschiedlichen Sicherheitsmerkmalen im Umlauf. Fingerabdrücke sind in zehn Ländern verpflichtend. In Deutschland können die Menschen selbst entscheiden, ob sie auf dem Ausweis ihre Fingerabdrücke hinterlegen wollen. Bei der Antragstellung muss für den elektronischen Personalausweis bisher lediglich ein Gesichtsbild geliefert werden, das als biometrisches Merkmal auf dem RFID-Chip des Dokuments gespeichert wird.

Die EU-Gremien einigten sich zudem gemäß dem Vorschlag der EU-Kommission auf optische Angleichungen: Alle Ausweise sollen im Kreditkartenformat ausgestellt werden und die europäische Flagge zeigen. Dazu kommen wird eine maschinenlesbare Zone. Insgesamt müssen die Mindeststandards für Sicherheit der Internationalen Zivilen Luftfahrtorganisation (ICAO) eingehalten werden.

Der Europäische Beauftragte für den Datenschutz Giovanni Buttarelli stellte zuvor in einem Gutachten fest, dass die Neuregelung bis zu 370 Millionen EU-BürgerInnen betreffen könnte; angesichts dieser Zahlen müsse das Datensammeln besonders gut begründet werden. Das aber geschehe im Entwurf nur unzureichend. Die Europäische Grundrechteagentur (FRA) wies darauf hin, dass die Grenzschutzagentur Frontex in den Jahren 2013 bis 2017 lediglich knapp 39.000 gefälschte Personalausweise ermittelt hat; die Zahl derjenigen, die mit gefälschten Papieren aus Drittländern einreisen wollten, sei rückläufig. Die Kommission selbst hatte in ihrer Folgenabschätzung, die mit jedem Gesetzesvorschlag veröffentlicht wird, eine Kombination aus biometrischer Aufnahme des Gesichts und freiwilligen Fingerabdrücken für ausreichend erachtet.

Ältere Ausweise, die den Vorgaben nicht entsprechen, sollen spätestens nach zehn Jahren ungültig werden. Für über 70-Jährige gelten längere Übergangsfristen. Ausweise für Kinder, die ebenfalls mit Fingerabdrücken versehen werden müssen, sollen weniger als fünf Jahre gelten. Die neuen Vorgaben sollen nach zwei Jahren direkt in allen Mitgliedsstaaten in Kraft treten.

Zuvor war im Europäischen Parlament Widerstand gegen die geplante Verordnung angekündigt worden. Vor allem Abgeordnete der Grünen, der Sozialdemokraten und der Linken wollen, dass es weiterhin den jeweiligen Mitgliedstaaten überlassen bleibt, ob sie Fingerabdrücke verlangen oder nicht. Sylvia-Yvonne Kaufmann (SPD), die für die Sozialdemokraten im EU-Parlament die Verhandlungen zu dem Thema führt, sagte, sie unterstütze zwar europaweit höhere Sicherheitsstandards für Personalausweise. „Die verpflichtende Speicherung der Fingerabdrücke ist jedoch nicht verhältnismäßig und nicht notwendig.“ Ihr zufolge hätten die Innenminister bei dem Thema „über die Bande“ gespielt: „Schließlich ist es für die Innenminister letztlich bequemer, über die EU-Ebene Entscheidungen herbeizuführen, statt sich zu Hause in den Mitgliedstaaten der öffentlichen Diskussion zu stellen.“ Ebenso befürchtet der grüne EU-Abgeordnete Sven Giegold, dass damit die „Datensammelwut befeuert“ wird. Polizei und Sicherheitsbehörden in Europa verknüpften immer mehr Daten, wobei unklar bleibe, „wer warum auf Fingerabdrücke zugreift“. Aus Bürgerrechtskreisen wird befürchtet, dass faktisch eine biometrische Superdatenbank mit der Verknüpfung zahlreicher Informationssysteme im Sicherheitsbereich errichtet wird. Mit dem Verschmelzen der Datentöpfe dürfte ein „Bevölkerungs-Scanner“ entstehen, der je nach politischer Wetterlage gegen unliebsame Personengruppen eingesetzt werden könnte.

Rumänien Innenministerin Carmen Daniela Dan, die für die rumänische Ratspräsidentschaft die Verhandlungen leitete, lobte den Kompromiss: „Die neuen Regeln für Sicherheitsstandards für Ausweispapiere werden es uns erleichtern, Dokumentenbetrug und Identitätsdiebstahl aufzudecken und Terroristen und Kriminellen das Handwerk erschweren.“ Stephan Mayer (CSU), Staatssekretär im BMI, begrüßte die Regelung als „erheblichen Sicherheitsgewinn“. Auch Bundesinnenminister Horst Seehofer (CSU) erklärte die Einführung des Fingerabdrucks für „zwingend erforderlich“. Es gebe gemäß seinem Ministerium einen „zunehmenden Missbrauch echter Dokumente durch ähnlich aussehende Personen“. Die Daten sollen nicht zentral, sondern nur im Chip des Personalausweises gespeichert werden. Aus der SPD ist zu hören, dass diese Art der Speicherung ein Kompromiss gewesen sei. Eigentlich habe man, anders als der Koalitionspartner, Vorbehalte gegen den Fingerabdruck gehabt. Auch das Bundesinnenministerium spricht hier von einer „Ausgleichsmaßnahme“.

Die Grünen halten die Einführung der Pflicht-Abdrücke für „hochproblematisch“. Ihr Vize-Fraktionsvorsitzender Konstantin von Notz sagte, es handele sich „um eine drastische Überbietung der nationalen Rechtslage, die im

Gesetzgebungsverfahren auch schon hochumstritten und verfassungsrechtlich bedenklich war“. Im Jahr 2008 hatte die damalige SPD-Justizministerin Brigitte Zypries die Verpflichtung noch gekippt, weil sie ein „Eingriff in die Grundrechte der Menschen“ sei (vgl. DANA 2/2008, 75 f.).

Das Bundesinnenministerium meint dagegen, die verfassungsrechtlichen Bedenken seien ausgeräumt. Und der innenpolitische Sprecher der Union Mathias Middelberg erklärte: „Die Grünen sollten ihren reflexhaften Widerstand, den sie schon unter Otto Schily gegen diesen Vorschlag gehegt und gepflegt haben, aufgeben.“ Die Fingerabdrücke auf dem Reisepass, die bereits verpflichtend sind, seien gut geschützt (Beisel/Szymanski, Fingerabdrücke in Personalausweisen, SZ 20.02.2019, 1; Krempl, EU-Gremien einig: Fingerabdrücke in Personalausweisen werden Pflicht, www.heise.de 20.02.2019, Kurzlink: https://heise.de/-4313534; Beisel/Ludwig, 370 Millionen Mal Daumen drücken, SZ 11.02.2019, 2).

EU

Entry/Exit System kommt

Bayerns Innenminister Joachim Herrmann (CSU) forderte nach einer USA-Reise, nach amerikanischem Vorbild auch in Europa „ein umfassendes Registrierungssystem für alle Ein- und Ausreisen“ zu schaffen. Die EU brauche dringend ein solches Ein- und Ausreiseregister. Von Leuten, die mit Touristenvisum einreisen, „weiß heute kein Mensch, ob der nach drei Monaten auch irgendwo wieder ausreist oder wo er sich gerade aufhält.“ Das sei „schon aus Sicherheitsgründen unerträglich“. Herrmann wusste wohl nicht, dass die Europäische Union (EU) für den Schengen-Raum derzeit ein solches System aufbaut. Bereits Ende 2017 trat eine Verordnung über ein solches Entry/Exit System (EES) in Kraft. Demnach soll in der Regel bei Einreisenden, die nicht BürgerInnen von EU- oder anderen Schengen-Staaten sind und für kürzere Aufenthalte nach Europa kommen, ein Dossier mit Foto und persönlichen Daten angelegt werden. Auch die Ausreise wird dann darin registriert. Spätestens 2021 soll das EES an den Außengrenzen des Schengen-Raums im Einsatz sein. Anfang Februar 2019 einigten sich Kommission, Rat und Parlament der EU auf ein Konzept, wie das EES und andere europäische Datenbanken miteinander verknüpft werden sollen (Registrierter Exit, SZ 11.02.2019, 2; s. u.).

EU

Biometrie-Superdatenbank beschlossen

Das EU-Parlament hat am 16.04.2019 ein Prestigeprojekt von Ex-Bundesinnenminister Thomas de Maizière (CDU) und EU-Sicherheitskommissar Julian King befürwortet. Gemäß zwei beschlossenen Verordnungsentwürfen zur „Interoperabilität“ sollen sämtliche EU-Datenbanken in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung miteinander verzahnt werden. Zugleich kann die biometrische Überwachung der Bevölkerung und Einreisender deutlich ausgebaut werden.

Über ein Suchportal sollen das Schengen-Informationssystem (SIS) mit rund 80 Millionen Einträgen, das Visa-Informationssystem (VIS) und Eurodac, wo vor allem Fingerabdrücke von Asylsuchenden gespeichert werden, verknüpft werden. Hinzukommen sollen das neue Ein- und Ausreisesystem zur biometrischen Grenzkontrolle (Smart Borders, EES, s. o.) sowie das Europäische Reisegenehmigungssystem (ETIAS). Ermöglicht werden soll so ein Abgleich der vorhandenen Daten „mit einem einzigen Klick“. Grenzschutz und Polizei könnten künftig etwa Ausweise einfacher überprüfen, indem sie alle EU-Informationssysteme auf einem Bildschirm gleichzeitig abfragen.

Auch ein übergeordneter „Speicher für Identitätsdaten“ ist für Angehörige von Drittstaaten vorgesehen. Einfließen sollen Informationen wie Geburtsdatum, Passnummer, Fingerabdrücke oder digitale Gesichtsbilder. Dazu kommt ein „gemeinsamer Dienst“ für den Abgleich biometrischer Daten, mit dem anhand von Fingerabdrücken und Gesichtsbildern alle bestehenden Informationssysteme abgefragt werden können. Darüber hinaus soll ein „Detektor für Mehrfachidentitäten“ für eine „unverzügliche Kennzeichnung aller Personen“ sorgen, „die mehrere oder falsche Identitäten verwenden“.

Bürgerrechts- und Datenschutzorganisationen haben massive Bedenken gegenüber diesen Plänen. Die britische Organisation Statewatch sieht darin eine schleichende massive Ausweitung der Befugnisse der Sicherheitsbehörden, für die der Big-Brother-Vergleich nicht übertrieben sei. Die zivilgesellschaftliche Instanz hat daher eine Beobachtungsstelle im Netz eingerichtet, in der sie über den Fortgang informiert (www.statewatch.org/interoperability/eu-big-brother-database.htm). Der EU-Datenschutzbeauftragte Giovanni Buttarelli warnte vor einem Punkt in der Sicherheitsarchitektur, „an dem es kein Zurück gibt“. Mit dem weiteren Zusammenwachsen der skizzierten Datenbanken würden bisherige rechtliche Prinzipien wie die Zweckbestimmung abgeschafft. Eine zentrale Datenbank für Strafverfolger und Geheimdienste erhöhe das Missbrauchsrisiko – nicht nur durch Hacker, sondern auch durch rechtmäßige Nutzer. Der Gesetzgeber vermische die Grenzen zwischen Migrationsmanagement und dem Kampf gegen schwere Verbrechen und Terrorismus. Ähnlich haben sich die Datenschutzbeauftragten der EU-Länder zu Wort gemeldet. Der linke Bundestagsabgeordnete Andrej Hunko fürchtet gar, dass mit dem Verschmelzen der polizeilichen Datentöpfe ein „Bevölkerungs-Scanner“ entsteht. Schon jetzt nutzen immer mehr Sicherheitsbehörden die Möglichkeit, über das SIS Verdächtige grenzüberschreitend heimlich zu überwachen: Waren darin Anfang 2016 noch 69.520 Personen zur sogenannten verdeckten Fahndung eingetragen, war die Zahl bis zum Juli 2018 auf 144.742 gestiegen.

Mit diesem undurchsichtigen Instrument erfährt die ausschreibende Behörde etwa bei einer polizeilichen Verkehrskontrolle oder einem Grenzübertritt, wohin eine betroffene Person wann und mit wem gereist ist. Ermittler oder Geheimdienste können die Daten speichern und zu umfassenden Bewegungs- und Kontaktprofilen verdichten. Betroffene erfahren davon in der Regel nichts. Nicht zuletzt bekommen

dadurch auch viele der nach rechts abdriftenden Regierungen in Europa leichteren Zugriff und können regimekritische wie unliebsame Personen über Landesgrenzen hinweg verfolgen. Das von den EU-Gremien im Februar 2019 geschnürte Paket muss noch den Ministerrat passieren, was als Formsache gilt (Krempl, Schengen-Überwachung: EU-Parlament beschließt Biometrie-Superdatenbank, www.heise.de 16.04.2019, Kurzlink: https://heise.de/-4400779; Krempl, EU plant biometrische Superdatenbank, https://www.heise.de/select/ct/2018/18/1535696151919730).

EU

Unfalldatenspeicher soll Pflicht werden

Das Parlament der Europäischen Union (EU) hat dem Entwurf einer Verordnung zugestimmt, die sog. Blackboxes, die bei Unfällen dokumentieren, was im Fahrzeug passiert ist, in Kraftfahrzeugen (Kfz) zur Pflicht macht. Geht der Regelungsvorschlag auch durch den Ministerrat, dann müssen Auto-Hersteller ab Mai 2022 in neuen Modellen nicht nur Alkohol-Wegfahrsperren und Sensoren zur Müdigkeitserkennung einbauen, sondern auch Blackboxes für Unfälle. Die EU-Kommission argumentiert mit der Sicherheit. Im Jahr 2018 kamen ihren Angaben zufolge rund 25.000 Menschen auf Europas Straßen ums Leben. Das seien 25.000 zu viel. Mit technischer Hilfe soll die Zahl der Verkehrstoten reduziert werden.

Die Unfalldatenspeicher registrieren u. a. Geschwindigkeit und Einsatz der Bremsen. Gespeichert werden diese Daten im Falle eines Unfalls, zum Beispiel, wenn der Airbag ausgelöst wird. Fahrer bzw. Fahrzeughalter sollen gemäß dem Text des Verordnungsentwurfes nicht direkt identifiziert werden können. Der Unfalldatenspeicher sollte innerhalb eines geschlossenen Regelkreises betrieben werden, bei dem die gespeicherten Daten überschrieben werden. Die Systeme sollen zur Fahrer-Müdigkeitserkennung und -Aufmerksamkeitswarnung sowie zur fortgeschrittenen Fahrerablenkungswarnung nur die Daten kontinuierlich aufzeichnen und vorhalten, die im Hinblick auf die Zwecke der Erhebung oder anderweitigen Verarbeitung im Rahmen des geschlossenen Regelkreises notwendig sind.

Der deutsche Bundesdatenschutzbeauftragte Ulrich Kelber bezweifelte, dass hinreichende Vorkehrungen zur Wahrung der Anonymität vorgesehen sind und zeigte sich generell skeptisch, was das Aufzeichnen von Informationen aus Autos und die Transparenz hierzu angeht. Es bedürfe gesetzlicher Vorkehrungen, dass die Daten aus dem Fahrzeug nicht gegen den Fahrer bzw. Inhaber verwendet werden können. Dies sei bisher im Entwurf der Verordnung nicht gewährleistet. Die Vorgaben zum Datenschutz seien nur punktuell (Sachsinger, EU will Blackbox fürs Auto einführen, www.br.de 18.04.2019).

EU

Anonyme Echtheitsprüfung von Arzneimitteln

Am 09.02.2019 ging ein EU-weites Schutzsystem mit Sicherheitsmerkmalen für Arzneien an den Start. Danach ist vorgeschrieben, dass rezeptpflichtige Mittel von Herstellerseite einen Barcode auf der Verpackung tragen müssen, mit dem sich in der Apotheke per Scan – in Gegenwart der KundIn – die Echtheit überprüfen lässt. Ein Siegeletikett soll garantieren, dass Schachteln nicht schon aufgemacht oder Pillen umverpackt wurden. Mit dem neuen Scanner-Schutzsystem sollen gefälschte Medikamente erkannt werden. Manipulierte Arzneimittel sind ein Milliongeschäft.

Der Gesundheitsforscher, Gerd Glaeske, Professor am SOCIUM Forschungszentrum Ungleichheit und Sozialpolitik der Universität Bremen, hält den End-to-End-Code für sehr sinnvoll und hilfreich. Apotheken in Deutschland seien zwar eher selten von manipulierten Medikamenten betroffen. Problematisch sei aber der internationale Handel und Online-Handel – „mit Packungen, die ganz ähnlich aussehen, wie die der Hersteller". Auch bei Online-Apotheken müssen für rezeptpflichtige Medikamente eigentlich Rezepte eingereicht werden, so Glaeske: „Was diese Fälscher tun und was diese Versandstellen letztlich dem Kunden anbieten, ist, dass sie all diese Medikamente auch ohne Rezepte bekommen. Und das ist der erste Hinweis darauf, dass etwas nicht stimmen kann."

Bei dem neuen Code-Verfahren handelt es sich um ein zweistufiges System, über das aber keine Patientendaten weitergegeben werden. Die Echtheitsprüfung erfolgt über einen Industrieserver, der anonymisiert feststellt, ob dieser Code tatsächlich ein echter Industrie-Code ist. Dazu Glaeske: „Und insofern ist dort auch für den Datenschutz gesorgt. Ich halte das für eine geglückte Lösung." Panschern in Apotheken könne man damit allerdings nicht das Handwerk legen. Das neue Sicherheitssystem kann nicht verhindern, dass – wie im Fall eines Bottroper Apothekers, der in großem Stil Krebsmedikamente gepanscht und damit auch Menschenleben gefährdet hat – industriell hergestellte Originalmittel vom Apotheker in Rezepturen verarbeitet werden, die dann aber nicht den Rezepturen entsprechen, wie sie vom Arzt vorgesehen gewesen seien (Glaeske im Gespräch mit Welty, www.deutschlandfunkkultur.de 09.02.2019).

EU

Japans Datenschutz ist EU-adäquat

Die EU-Kommission beschloss mit Wirkung vom 23.01.2019, dass Japan einen dem europäischen Datenschutz-Standard entsprechenden Datenschutz hat, so dass einem Austausch zwischen dem Land und der EU keine regulativen Hindernisse entgegen stehen. Die Justizkommissarin der EU Vera Jourova erklärte am 22.01.2019 stolz: „Es wird der weltweit größte Raum für sicheren Datenverkehr geschaffen." Der Beschluss ist Bestandteil des Freihandelsabkommens zwischen Tokio und den 28 Mitgliedstaaten – Großbritannien gehört immer noch dazu. Für 508 Millionen Menschen in Europa plus 127 Millionen in Japan gelten vergleichbare Bestimmungen. Wenn demnächst Strafverfolgungsbehörden auf der fernöstlichen Insel Daten von europäischen Staatsbürgern abrufen, dürfen sie diese – genau wie innerhalb der EU – ausschließlich

für klar umrissene Verdachtsmomente nutzen. Der Zugriff muss „erforderlich und verhältnismäßig" sein. Ohne Einwilligung der Betroffenen dürfen Informationen auch nicht von japanischen Behörden an Drittländer weitergeleitet werden. Zusätzliche Garantien, welche die japanische Regierung übernehmen musste, betreffen den Schutz personenbezogener Daten von EU-Bürgern wie etwa die sexuelle Orientierung oder politische Ausrichtung.

Der Datenschutz wird als Begleitinstrument für die Umsetzung des japanisch-europäischen Freihandelsabkommens (Jefta) gebraucht. Dieser Vertrag wurde bereits am 17.07.2018 unterzeichnet. Er öffnet die Türen nicht nur für einen weitgehend zollfreien Handel, sondern auch für digitale Dienstleistungen und Finanzinformationen. Überall dort fallen personenbezogene Informationen an, die aber den europäischen Standards unterliegen. So bleiben die Rechte der EU-BürgerInnen an ihren Daten auch dann erhalten, wenn sie in Japan genutzt werden. Für den Fall, dass es zum Missbrauch kommen sollte, hat Tokio mit der Personal Information Protection Commission (PCC) eine unabhängige Aufsichtsbehörde geschaffen, die ähnlich wie in Deutschland die Landes- und Bundesbeauftragten für Datenschutz bei Einsprüchen zuständig ist.

Der Adäquanzbeschluss zu Japan geht über das für den Transfer zwischen der EU und USA geltende „Privacy Shield" hinaus. Die EU macht damit gegenüber weiteren möglichen Partnern künftiger Freihandelsverträge wie beispielsweise den Staaten des asiatisch-pazifischen Raums klar, dass alle Vereinbarungen mit Europa nicht hinter diesen Datenschutz-Standard zurückfallen dürfen. Derart ist die Datenschutz-Grundverordnung auf dem Weg, zu einem globalen Standard zu werden, zumindest für jene, die sich als Partner Europas verstehen. Für die Unternehmen, so betonte die Kommission, sei dies ein „großer Vorteil": Schließlich könnten sich alle, die mit Japan und mit der EU Geschäfte machen, auf die gleichen Schutzvorschriften einstellen. Das werde den Handel erleichtern und in den Betrieben Klarheit schaffen (Drewes, Japan übernimmt europäische Datenschutz-Standards. www.noz.de 23.01.2019).

Österreich

Löschen ist auch Anonymisieren, nicht nur Vernichten

Gemäß einer Entscheidung der österreichischen Datenschutzbehörde (DSB) genügt es für die Umsetzung des in der Datenschutz-Grundverordnung (DS-GVO) verbrieften Rechts auf Löschung personenbezogener Daten, dass die Daten anonymisiert werden, d. h. dass der Personenbezug aus einem Datensatz entfernt wird. Im Juli 2018 hatte ein Österreicher von seiner ehemaligen Versicherung verlangt, alle über ihn gespeicherten Daten unverzüglich zu löschen. Die Versicherung löschte E-Mail-Adresse, Telefonnummer sowie Angaben über ein einst erbetenes Versicherungsangebot und stoppte alle Werbezusendungen. Name und Adresse wurden allerdings durch „Max Mustermann" mit einer Musteradresse ersetzt, und Informationen über zwei frühere Versicherungsverträge blieben offenbar erhalten. Eine endgültige Vernichtung aller Daten wurde erst für März 2019 in Aussicht gestellt. Der Kunde bestand aber auf einer sofortigen Löschung und beschwerte sich bei der Datenschutzbehörde, die zugunsten der Versicherung entschied (Az. DSB-D123.270/0009-DSB/2018).

Artikel 17 DSGVO gewährt ein Recht auf Löschung personenbezogener Daten. Artikel 4 Nr. 2 DSGVO weise darauf hin, dass Löschung und Vernichtung nicht identisch seien, da beide Begriffe nebeneinander aufgeführt werden. Es liege im Ermessen des Verantwortlichen der Datenverarbeitung, die Löschmethode zu bestimmen: „Es muss jedoch sichergestellt werden, dass weder der Verantwortliche selbst, noch ein Dritter, ohne unverhältnismäßigen Aufwand einen Personenbezug wiederherstellen kann." Der Versicherung hat in diesem Fall geholfen, dass sie auch keine Logdateien mehr hatte, über die die Anonymisierung wieder hätte ausgehebelt werden können. Die Behörde forderte nicht, dass die Anonymisierung niemals rückgängig gemacht werden kann: „Eine Löschung liegt dann vor, wenn die Verarbeitung und Nutzung der personenbezogenen Daten (...) nicht mehr möglich ist. Dass sich zu irgendeinem Zeitpunkt eine Rekonstruktion (etwa unter Verwendung neuer technischer Hilfsmittel) als möglich erweist, macht die ‚Löschung durch Unkenntlichmachung' nicht unzureichend. Eine völlige Irreversibilität ist daher (...) nicht notwendig" (Sokolov, Datenschutz in Österreich: Löschen heißt nicht unbedingt vernichten, www.heise.de 11.02.2019, Kurzlink: https://heise.de/-4303367).

Österreich

Regierung plant „digitales Vermummungsverbot" im Netz

Die Bundesregierung in Österreich will mit einem Gesetz gegen Hass im Netz vorgehen. Das umstrittene Projekt zielt darauf ab, die Anonymität im Netz einzuschränken. Justiziable Hass-Postings sollen strafrechtlich besser verfolgt werden können. Anwendbar sollen die Pläne insbesondere auf soziale Netzwerke sowie Zeitungsforen sein, deren Nutzende sich noch nicht identifizieren müssen.

Der Entwurf wurde am 10.04.2019 im Ministerrat (so heißt in Österreich das Bundeskabinett) behandelt und abgesegnet. Regierungsintern läuft das im Kanzleramt ausgearbeitete Projekt als „digitales Vermummungsverbot": Die User können demnach weiter unter Pseudonym posten, doch die Plattformen müssen die Identität der Nutzer kennen und sie gegebenenfalls an Strafverfolgungsbehörden herausgeben. Dem Vernehmen nach dürfte es auf eine Registrierungspflicht per Handynummer hinauslaufen. Mit dem Gesetz soll laut Medienminister Gernot Blümel (ÖVP) verhindert werden, dass sich Menschen bei Straftaten „in der Anonymität des Internets verstecken können". Was in der analogen Welt geahndet werde, müsse auch Folgen in der digitalen Welt haben.

Die Pläne zielen auf Seiten, die auf den Alpenstaat ausgerichtet sind, mit mehr als 100.000 Nutzenden, Seiten mit einer Presseförderung von mehr als 50.000 Euro in einem Kalenderjahr sowie Seiten mit einem in Österreich erzielten Umsatz von mehr als 500.000 Euro pro Jahr. Neben Nachrichtenwebsi-

tes wie „Der Standard" und „Die Presse" wären fast alle großen US-Plattformen wie Facebook, Twitter und YouTube betroffen – Seiten, auf denen die Nutzenden bisher meist nur Namen und E-Mail-Adressen hinterlegt haben.

Sollte dem Gesetz zugestimmt werden, müssten die Tech-Konzerne künftig die Adressen der österreichischen Nutzenden sammeln und per Ausweis-Check oder mit einem ähnlichen Verfahren überprüfen. Wer sich als Websitebetreiber nicht daran hält, soll mit Bußgeldern von bis zu einer Million Euro bestraft werden. Ausgenommen von der Sammelpflicht werden Onlineplattformen, auf denen Waren verkauft oder getauscht werden. Wie betroffene Unternehmen ihre Dienste im Detail umgestalten würden, damit sie dem Gesetz entsprechen, ist unklar. Facebook, Google und Twitter haben hierzu auf Anfrage bisher keinen Kommentar abgegeben.

Unter den Zeitungsforen würde die künftige Regelung sich vor allem auf den regierungskritischen „Standard" auswirken. Dessen Diskussionsplattform ist die größte Österreichs mit bis zu 40.000 Kommentaren am Tag. In der Redaktion stößt die Initiative auf Unverständnis, so Gerlinde Hinterleitner, Community-Leiterin beim Standard: „Shitstorms und Hass-Postings finden in der Regel nicht bei uns statt, eher bei Facebook und Twitter" Dies sei so, obwohl die meisten dort nicht unter Klarnamen posten und nicht immer nachvollziehbar ist, wer hinter den Äußerungen steckt. Gegen Störenfriede gehe man sofort vor.

Bei der Kronen-Zeitung, dem auflagenstärksten Blatt in Österreich, äußert man dagegen Verständnis für den Plan der Regierung. Michael Eder, Geschäftsführer der digitalen Krone, schlägt allerdings einen weiteren Schritt vor: „Um den Schutz der Daten jedes Einzelnen sicherzustellen, plädieren wir für eine zentrale Clearingstelle". Diese Stelle könnte sicherstellen, „dass jene Daten, die zur Ausforschung betroffener Personen dienen können, nicht in unseren Händen, sondern von einer unabhängigen Institution zentral gespeichert und verwaltet werden und nur per Gerichtsbeschluss erhoben werden dürfen."

Der österreichische IT-Anwalt Walter Korschelt sagte, er begrüße zwar, dass etwas gegen Hasskommentare im Netz unternommen werde. Doch die Hürde, sich samt Adresse bei Onlineportalen anzumelden, gelte eben nicht nur für beleidigende Nutzende, sondern für alle Menschen in Österreich. Der Rechtsexperte hält die Identifizierungspflicht für fragwürdig: „Wenn ich im echten Leben meine Meinung äußere, muss ich vorher auch nicht meinen Ausweis vorlegen." Korschelt kritisiert, dass mit dem Gesetz zu viel Verantwortung an Facebook und Co. übertragen werde. Denn laut dem Entwurf sollen nicht nur Behörden bei Bedarf Adressen anfordern können, sondern auch Privatpersonen. Die Bedingung: Der Antragsteller muss nachweisen können, dass er einen Nutzer aufgrund eines Kommentars anzeigen möchte. „Der Staat verlagert die Aufgabe der Gerichte, herauszufinden, ob etwas strafbar ist, auf private Dienstleister aus." Das könne dazu führen, „dass auch private Daten herausgegeben werden, die strafrechtlich nicht relevant sind". Man müsse abwarten, ob das mit der EU-Datenschutzgrundverordnung (DSGVO) vereinbar sei. Denn darin stehe, so Korschelt, dass grundsätzlich so wenige Daten wie nötig gesammelt werden sollen.

Bürgerrechtler des österreichischen Vereins Epicenter Works gehen noch einen Schritt weiter. Sie sehen in dem Gesetz einen „Frontalangriff auf das Mitmach-Internet": „Dieses Gesetz verfehlt sein eigentliches Ziel und bringt einen enormen Kollateralschaden für unseren demokratischen Diskurs." Whistleblower und Minderheiten würden dadurch bedroht, dass ihr Name und ihre Anschrift für Privatanklagedelikte an Dritte herausgegeben werden müssten.

Der Plan für ein „digitales Vermummungsverbot" war von der konservativen ÖVP von Bundeskanzler Sebastian Kurz forciert worden. Bei seinem Koalitionspartner FPÖ war man wenig begeistert. Die Rechtspopulisten profitieren seit Jahren davon, dass ihre Anhängerschaft im Netz anonym Stimmung macht. Die angedachte Gegenmaßnahme sorgte vorab für so manchen internen Widerspruch von FPÖ-ParlamentarierInnen. Doch FPÖ-Vizekanzler Heinz-Christian Strache hatte schon zuvor seine Zustimmung gegeben. Die Pläne gegen vermeintliche Anonymität im Internet hatte die rechtskonservative Regierung aus ÖVP und FPÖ im November 2018 vorgestellt. Erklärtes Ziel war es demnach, „den Umgang im Netz respektvoller" zu machen. Zuvor hatte ein Fall in dem Land für Aufsehen gesorgt, in dem es um obszöne Facebook-Nachrichten an die Grünen-Politikerin Sigi Maurer und deren Veröffentlichung sowie die Benennung des Absenders durch die Betroffene ging. Die Hassposts waren aber unter Klarnamen versendet worden. Es wäre, so Maurer, deshalb wichtiger, die Möglichkeiten zur Gegenwehr zu erweitern (dazu s. u. S. 112 Urteil des OLG Wien).

Der umstrittene Entwurf wurde sechs Wochen lang zur Begutachtung freigegeben. In dieser Zeit sind Stellungnahmen möglich. Anschließend werden mögliche Änderungen eingearbeitet, bevor der Nationalrat, in dem die Regierung die Mehrheit hat, über das Gesetz abstimmt. Schließlich entscheidet der Bundesrat über den Entwurf, was aber als Formsache gilt.

Es ist zweifelhaft, dass das geplante Gesetz zu weniger Hetze führt. Eine ähnliche Initiative in Südkorea, die Nutzenden Identifikationsnummern zuteilte, senkte die Zahl der Verbalattacken nur vorübergehend. Dann änderten sich die Beschimpfungen: Sie wurden auf nicht justiziable Weise formuliert. Südkoreas oberstes Gericht hielt das Gesetz schließlich für als zu weitgehend und gleichzeitig für ineffizient und hob es auf (Das Gupta, Maßnahme gegen Hass-Kommentare Österreich bekommt „digitales Vermummungsverbot", www.sueddeutsche.de 08.04.2019; Holland, Österreich: „Digitales Vermummungsverbot" soll nun wohl kommen, www.heise.de, Kurzlink: https://heise.de/-4365622; Breithut, Nutzer von Plattformen wie Facebook sollen private Adressen angeben, www.spiegel.de 12.04.2019).

Schweiz

EU kritisiert Ausstattung beim Datenschutz

Anlässlich der regelmäßigen Überprüfung, inwieweit die Schweiz als Schengen-Mitglied die Schengen-Regeln einhält, stellte der EU-Ministerrat in ei-

nem Bericht fest, dass beim Datenschutz Defizite bestehen: zu wenig Personal und zu wenig Kompetenzen. Der Bericht gibt Beat Rudin, Präsident der kantonalen Datenschützer, der schon lange für mehr Ressourcen kämpft, Aufwind: „Wir hoffen, dass sich jetzt das Ganze beschleunigt, weil die EU festgestellt hat, dass die Ausgestaltung der Datenschutzaufsicht nicht genügt." Die kantonalen Datenschutzstellen, die wie in gewissen kleinen Kantonen nur aus einer 20%- oder 30%-Stelle bestehen, müssten personell aufgerüstet werden; ansonsten hätten sie zu kurze Spieße im Kampf gegen Datenklau im Internet. Der EU-Ministerrat fordert die Schweiz zudem auf, die Befugnisse der Datenschützer zu erweitern. Heute können sie nur Empfehlungen abgeben, neu sollten die kantonalen und der nationale Datenschützer aber auch verbindliche Verfügungen erlassen können. Dadurch bekämen sie deutlich mehr Macht, so Rudin.

Für ihn ist klar, dass der EU-Bericht Folgen haben wird: „Wenn diese Schengen-Evaluation nicht erfüllt wird, dann riskiert die Schweiz die Aufhebung der Schengen-Assoziierung. Beispielsweise unsere Polizei hätte überhaupt keine Freude daran, wenn sie den Zugang zum Schengener Informationssystem nicht mehr hätten." Mehr Mittel und mehr Macht seien nötig, damit die Datenschützer auch in Zukunft ihrer Aufgabe nachkommen – nämlich die Daten der Bürger zu schützen. Der Eidgenössische Datenschutzbeauftragte Adrian Lobsiger schloss sich umgehend den Forderungen der kantonalen Datenschützer an (von Matt, Datenschutz in der Schweiz - EU kritisiert die Schweiz – und die Datenschützer freut es, www.srf.ch 28.03.2019).

Slowakei

Multimillionär des Mordes und der Journalistenbespitzelung beschuldigt

Der Geschäftsmann Marian Kočner ist der mutmaßliche Auftraggeber des Mordes an dem 27-jährigen Journalisten Ján Kuciak am 25.02.2018. Gegen Kočner wurde deshalb von der Staatsanwaltschaft Anfang 2019 Anklage erhoben. Ihm wird auch vorgeworfen, von Anfang 2017 bis Mai 2018 systematisch Journalisten ausgespäht zu haben, darunter auch den ermordeten Kuciak. Mindestens sechs Leute spannte Kočner dafür ein, darunter einen Ex-Geheimdienstagenten namens Peter Tóth. Der hat laut dem Protokoll eines Polizeiverhörs erklärt, er sei davon ausgegangen, Kočner brauche die Informationen für seine Facebook-Seite, auf der er regelmäßig Schmähungen über Journalisten verbreitete, die kritisch über ihn berichteten.

Vier Monate, bevor er zusammen mit seiner Verlobten erschossen wurde, hatte Ján Kuciak Anzeige gegen Marian Kočner erstattet, weil er sich von ihm bedroht fühlte. Dieser hatte ihm gedroht: „Ich werde anfangen, Herr Kuciak, mich für Ihre Mutter zu interessieren, für Ihren Vater, für Ihre Geschwister, ich werde mich um sie alle kümmern, und ich werde alles veröffentlichen, was ich über Sie finde, Herr Kuciak." Die Polizei wies den Reporter ab: Was er schildere, sei nicht einmal ein Bagatelldelikt.

Gemäß einem Pressebericht prahlte Kočner drei Monate vor dem Mord an Kuciak in einer von Ermittlern abgefangenen SMS, er habe bis dato 200.000 Euro für die Bespitzelung von Journalisten ausgegeben. Er wisse nun, wer mit wem Beischlaf pflege, „wer eine Schwuchtel ist, ein Säufer, ein Tyrann. Komplett mit Bildern und Videodokumentation." Bei diesem so akribisch gepflegten Projekt kamen dem Multimillionär mutmaßlich seine Kontakte in die Sicherheitsbehörden zugute. Dem Bericht zufolge ermittelt die Polizei gegen einen früheren Abteilungsleiter der Finanzpolizei, weil dieser an der Ausspähung von Ján Kuciak beteiligt gewesen sein soll. Der hat demnach ausgesagt, er habe den Auftrag dazu vom damaligen Polizeipräsidenten Tibo Gašpar erhalten, was dieser bestreitet, der aber zugleich weiter ins Zwielicht gerät: Unter Berufung auf übereinstimmende Informationen von Europol und anderen Behörden berichtete der italienische Fernsehsender Rai Uno, Gašpar habe bereits 2013 davon gewusst, dass ein italienischer Geschäftsmann namens Antonino Vadalà dabei war, im Osten der Slowakei eine Zelle der kalabrischen ´Ndrangheta aufzubauen. Kuciak hatte vor seinem Tod zu Vadalà und dessen Beziehungen in höchste Regierungskreise recherchiert. Kurz nach Kuciaks Ermordung erklärte Gašpar, der slowakischen Polizei lägen keine Informationen über derartige ´Ndrangeta-Umtriebe in ihrem Land vor – eine Aussage, die der Rai-Bericht widerlegt (Zick, Kuciak war nicht der einzige, SZ 26.04.2019, 7).

USA

Apps melden Facebook ungefragt sensitive Gesundheitsdaten

In den USA berichteten Medien am 22.02.2019, dass etliche Smartphone-Apps vor allem aus dem Gesundheitsbereich private Informationen der Benutzenden ohne deren Zustimmung zu Werbezwecken an Facebook senden. Der Gouverneur des US-Bundesstaats New York leitete hierzu umgehend eine Untersuchung ein. Ein erster App-Hersteller veröffentlichte darauf ein Update, in dem das kritisierte Vorgehen abgestellt sein soll. Derweil weist Facebook eine Mitschuld an den Vorgängen zurück.

Als entsprechend programmierte Apps wurde u. a. die App Flo genannt, mit der Frauen ihre Menstruation und ihren Eisprungzyklus überwachen und Hilfe bei einem Schwangerschaftswunsch erhalten können. Die App HR Monitor zur Messung der Herzfrequenz soll diese ebenso an Facebook gemeldet haben wie die Immobilien-App Realtor die Besichtigung einer Immobilie, an deren Kauf die BenutzerIn interessiert ist. Zu weiteren übermittelten persönlichen Daten gehören Blutdruck und Gewicht der Benutzenden oder die Nutzung einer Meditations-App. Die App-Entwickler nutzten dabei Software von Facebook, mit der über ein „Custom Event" genanntes Feature ein Ereignis in der App das Übertragen entsprechender Daten an den Social-Media-Konzern auslöst, zusammen mit einer eindeutigen Werbe-ID, die sich dem Report zufolge mit einem Gerät oder einem Profil verknüpfen lässt.

Die Daten wurden offenbar ohne Wissen und Zustimmung der Benutzenden zum Zweck der Werbung an Facebook übertragen – und zwar nicht nur bei

Benutzenden mit Facebook-Konto, sondern auch, wenn diese sich in der jeweiligen App nicht bei Facebook angemeldet hatten. Übermittelt wurden selbst Daten, wenn die Benutzenden gar kein Konto bei Facebook besitzen. Eine Möglichkeit, die Datenweitergabe in den Apps zu unterbinden, soll nicht bestanden haben. Der Test umfasste ungefähr 70 mehr oder weniger populäre Apps in Apples App Store, von denen 11 entsprechende Daten übermittelten. Android-Versionen existieren von mehreren Apps, die aber nicht getestet worden sind.

Der Gouverneur des US-Bundesstaats New York Andrew Cuomo nannte die Datenübertragung an Facebook einen „ungeheuerlichen Missbrauch der Privatsphäre" und beauftragte zwei ihm unterstellte Behörden mit einer Untersuchung der Vorgänge. Außerdem rief Cuomo die zuständigen Regulierungsbehörden des Bundes auf, ebenfalls tätig zu werden. Facebook erklärte, es wolle die New Yorker Behörden bei der Aufklärung unterstützen. Das Social-Media-Unternehmen verwies darauf, dass die Entwickler der Apps die Einwilligung der Benutzer für eine Datenübermittlung einholen müssten, und dass Facebook den Entwicklern untersage, sensible persönliche Daten (etwa aus dem Gesundheitsbereich) zu übermitteln. Das Unternehmen bemühe sich, Daten zu finden und zu löschen, die es nicht hätte erhalten dürfen. Cuomo hatte zuvor Ende Januar 2019 gemeinsam mit der Generalstaatsanwältin Letitia James gegen Apple wegen eines schwerwiegenden Datenschutz-Bugs in der Gruppenchat-Funktion von FaceTime Ermittlungen eingeleitet.

Der Entwickler der Menstruations-App Flo, Flo Health, äußerte sich zu der Angelegenheit. Die Datenübertragung soll in einer aktualisierten Version der App – für iOS und Android – abgestellt werden. Damit habe man jegliche Datenübertragung an andere Unternehmen abgestellt, so der Entwickler. Die Firma wolle sich zudem einer Datenschutzprüfung unterziehen. Das unkontrollierte Datensammeln war zuvor insbesondere bei Android-Apps mehrfach ans Licht gekommen, so etwa das Erfassen von Standortdaten trotz des Widerspruchs der Benutzenden, das Vorhandensein von Tracker-Skripten zum Erheben von Nutzungsdaten oder das tausendfache Umgehen der Werbe-ID (Wittenhorst, Apps liefern Facebook vertrauliche Daten – Untersuchung angekündigt, www.heise.de 24.02.2019; Kurzlink: https://heise.de/-4316943).

USA

Family Tree unterstützt freiwillig FBI

Eines der größten Unternehmen für private DNA-Tests, Family Tree DNA, hat zugegeben, dem FBI freiwillig die Nutzung der eigenen DNA-Datenbank zu gestatten. Das US-amerikanische Unternehmen wolle damit beim Aufklären von Kriminalfällen helfen. Das FBI könne nicht frei in der Datenbank von Family Tree DNA suchen. Die Firma nehme seit Herbst 2018 DNA-Proben auf Basis einzelner Fälle entgegen und gleiche diese – ohne Kenntnis ihrer Kunden – mit der Datenbank ab. Einen Vertrag mit dem FBI über diese Zusammenarbeit gebe es nicht, doch hat das Unternehmen im Dezember 2018 seine Geschäftsbedingungen entsprechend angepasst.

Eine Sprecherin des Unternehmens teilte mit, dass dieses dem FBI bis Januar 2019 in weniger als 10 Fällen geholfen habe. Beim Abgleich mit der Datenbank könnten direkte Treffer oder auch Verwandtschaftsbeziehungen zur vorliegenden DNA-Probe ermittelt werden. Durch die Zusammenarbeit hat das FBI indirekt Zugriff auf mehr als eine Million DNA-Profile von Privatpersonen, die ihre genetischen Informationen dem Unternehmen anvertraut haben. Family Tree DNA nimmt bereits vorhandene Gen-Informationen entgegen und verkauft auch Sets, mit denen KundInnen eine Genprobe nehmen und zur Analyse zurücksenden können.

Das Unternehmen rechtfertigte die Zusammenarbeit mit dem FBI damit, dass man mit der eigenen Plattform helfen könne, Kriminalfälle schneller als je zuvor zu lösen. Außerdem könnten KundInnen per Opt-out dem Auffinden ihrer Gendaten widersprechen. Ein nicht mehr auffindbarer Eintrag würde jedoch dem ursprünglichen Zweck der Datenbank widersprechen, darüber etwa Verwandtschaftsbeziehungen aufzuklären. Family Tree DNA sieht auch nicht seine Privatsphäre-Bestimmungen verletzt. Die Zusammenarbeit mit dem FBI sei in etwa so, als würde die Behörde ein Nutzerkonto bei der Firma anlegen und mit einem eigenen DNA-Profil nach Treffern suchen. Im Jahr 2017 war der Mutterkonzern von Family Tree DNA per Gerichtsbeschluss verpflichtet worden, Informationen zu dem als „Golden State Killer" bekannt gewordenen Kriminalfall herauszugeben (Wittenhorst, DNA-Analysefirma gestattet FBI Nutzung des Datenbestands, www.heise.de 02.02.2019, Kurzlink: https://heise.de/-4296628; vgl. DANA 2/2018, 116 f.).

USA

23andMe informiert ungefragt über genetisches Typ-2-Diabetes-Risiko

23andMe, ein Unternehmen aus dem Silicon Valley, das DNA-Tests direkt an VerbraucherInnen vermarktet, wirbt mit dem Motto „Jeder hat ein Recht auf seine genetischen Informationen." Es hat eine Krankheitsvorhersage auf den Markt herausgebracht, bei der aus einer DNA-Analyse das genetische Risiko beauskunftet wird, dass eine Person Typ-2-Diabetes bekommen wird. Im März 2019 sollen mehrere Millionen KundInnen diese Information durch das Unternehmen erhalten haben. Die Analyse basiert auf einem polygenetischen Risikowert, bei dem DNA-Informationen im gesamten Genom berücksichtigt werden. Im Fall des neuen Diabetes-Tests werden laut 23andMe Informationen von 1.244 unterschiedlichen Stellen im Genom eines Menschen untersucht, wobei jede davon einen kleinen Anteil an der Gesamt-Risikobewertung habe.

Ungefähr 80% der KundInnen würden so erfahren, dass ihre persönliche DNA ein durchschnittliches Risiko für sie bedeutet, bei 20% bestünde eine erhöhte Diabetes-Wahrscheinlichkeit. Nur die Personen in der Gruppe mit höherem Risiko erhalten das genauere Berechnungsergebnis (zum Beispiel eine Wahrscheinlichkeit von 3 zu 5 über das gesamte Leben gesehen). Diese Berichtsart stieß auf starke Kritik. Polygenetische

Bewertungen seien zwar viel versprechend, aber nicht sehr exakt, sie brächten zudem keine belegten Vorteile für die Gesundheit, so Peter Kraft, ein Epidemiologe an der School of Public Health der Harvard University: „Ich halte das für ein riesiges Experiment. Es wird für Millionen Menschen angeboten, aber es gibt noch viel, was wir nicht wissen."

Anfang März 2019 stellte 23andMe Medien einen exemplarischen Bericht zur Verfügung, für einen imaginären Kunden lateinamerikanischer Herkunft namens Jamie. Demnach besteht für Jamie eine sehr hohe Wahrscheinlichkeit, im Lauf seines Lebens Diabetes zu bekommen. Anschließend wird ihm empfohlen, für 19,99 Dollar im Monat eine Coaching-App namens Lark auszuprobieren, die von einem Partner von 23andMe angeboten wird. Grundlage für die Risiko-Berichte seien neue wissenschaftliche Erkenntnisse. Mit DNA von genügend Menschen ist es inzwischen möglich, statistische Modelle zu entwerfen, die anhand der DNA von einzelnen Personen Voraussagen für deren wahrscheinliche Merkmale erlauben. Möglich ist das außer für Diabetes zum Beispiel für Brustkrebs, eine besonders geringe Körpergröße oder einen überdurchschnittlichen Intelligenzquotienten (IQ). Im Jahr 2018 wurden mindestens 216 wissenschaftliche Aufsätze zu solchen polygenetischen Risikowerten veröffentlicht. Das Konzept schaffte es auf die Liste der 10 bahnbrechenden Technologien 2018.

Für seine Diabetes-Prognosen hat 23andMe nach eigenen Angaben seine enorme Sammlung an DNA-Daten genutzt und mehr als 70.000 KundInnen analysiert, die angaben, unter Typ-2-Diabetes zu leiden; hinzu kamen mehrere Millionen, bei denen das nicht der Fall war. Für das Unternehmen ist das Potenzial dieser Scoring-Technologie erheblich. In einem Förderantrag bezeichnet es „hochgradig skalierbare und genaue Einschätzungen von Krankheitsrisiken" als die „nächste Phase" seiner Forschungsarbeit. Ob Risiko-Berichte auch für andere Krankheiten geplant sind, wollte 23andMe nicht sagen.

Im Jahr 2013 zwang die US-Regierung das Unternehmen, eine lange Liste von Gesundheitstests zurückzuziehen, weil deren Genauigkeit nicht hinreichend belegt wurde und weil sie Menschen dazu bringen könnten, unnötige medizinische Maßnahmen zu ergreifen. Viele der Tests wie der auf Typ-2-Diabetes basieren auf polygenetischen Indikatoren. Seitdem die Forschung Fortschritte gemacht hat, ist die Regulierung in den USA lockerer geworden. Laut 23andMe gibt es für den neuen Diabetes-Tests keinerlei regulatorische Vorgaben. Denn er fällt unter eine Ausnahmeregelung für Tests mit geringem Risiko und Telefon-Apps, die nur Empfehlungen zu „allgemeiner Wellness" bieten, keine echte medizinische Beratung oder Diagnosen.

Dazu kritisch Cecile Jansen, eine Epidemiologin an der Emory University: „Dass sie diesen Weg gehen würden, war absolut abzusehen. Es ist zwar noch viel zu früh, diese Art von Informationen zu verbreiten, aber 23andMe findet, dass das keine Rolle spielt, solange man ehrlich auf die Schwächen hinweist." Besonders lückenhaft sind die genetischen Prognosen für Afroamerikaner, da das Modell von 23andMe weitgehend auf DNA von weißen Menschen europäischer Abstammung basiert, die den Großteil seiner Datenbank ausmachen. Die Folge davon ist, dass die Voraussagen für andere Bevölkerungsgruppen weniger Aussagekraft haben (Regalado, DNA-Test auf Typ-2-Diabetes, www.heise.de 18.03.2019).

USA/China

Keine DNA-Analysetechnik mehr für Ethno-Unterdrükkung in Xinjiang

Das US-Technologieunternehmen Thermo Fisher mit Sitz in Massachusetts stellt die Lieferung von Geräten an die chinesische Regional-Regierung von Xingjang ein, mit denen eine DNA-Datenbank der Minderheit der Uiguren erstellt wird. Das Sammeln, Archivieren und Auswerten von DNA ist Teil eines umfassenden Überwachungs- und Kontrollprogramms der chinesischen Regierung in der Region Xinjiang, die mehrheitlich von moslemischen Uiguren bewohnt wird. Dabei wurde Technik von Thermo Fisher eingesetzt.

Chinesische Stellen beteiligen sich an weltweiten Projekten zur DNA-Analyse. Thermo Fisher war nach eigenem Bekunden zunächst nicht bewusst, in welcher Weise die gelieferte Technik zum Einsatz kommt und bat deshalb offizielle US-Stellen, das Unternehmen bei der Recherche über den Technikeinsatzes in China zu unterstützen. Mark Munsterhjelm, Professor an der University von Windsor/Ontario, untersuchte den Einsatz der Technik in Xinjiang und meinte, dass die weltweit stattfindenden Kooperationen „diese Form der genetischen Überwachung legitimiert". Die Regierung von Xinjiang bestritt hingegen, dass DNA-Proben als Teil eines Gesundheitsprogramms gesammelt würden. Die Analysetechnik sei von den Behörden für „interne Zwecke" beschafft worden.

Die genetische Kooperation zwischen den USA und China basierte ursprünglich auf wissenschaftlichem Interesse. 2010 besuchte Kenneth Kidd, ein angesehener Yale-Professor, das Land und entwickelte in den folgenden Jahren eine Forschungszusammenarbeit, in deren Verlauf auch Chinesen in seinen US-Laboren tätig waren. 2013 und 2017 veröffentlichten chinesische offizielle Forschende Patente zur Feststellung der ethnischen Herkunft, wobei als Referenzgruppen Uiguren und Inder dienten. Es zeigte sich, dass die Referenzdaten aus dem 1000-Genomes-Project stammten, an dem Kidd beteiligt war. Die chinesischen Forschenden steuerten ihrerseits für internationale Forschung Datensätze von 2.143 UigurInnen bei. Der 77-jährige Kidd erklärte, „nicht besonders glücklich" zu sein, dass seine Daten in einer Weise genutzt worden sind, die nicht den Betroffenen diene. Er könne die Chinesen hiervon aber nicht abhalten. Er sei sich über diese Verwendung auch nicht bewusst gewesen: „Ich ging davon aus, dass die Proben auf Grundlage einer informierten Einwilligung beschafft wurden. Erst vor kurzem habe ich davon erfahren, dass die Behandlung von Uiguren bedenklich ist." Ein weiterer US-Wissenschaftler, der mit China kooperierte, war Bruce Budowle, Professor der University of North Texas. Kidd und Budowle waren Gastredner einer 2015 in Xi´an/China durchgeführten Konferenz über Gentechnik, die u. a. von Thermo Fisher organisiert worden war. Das Unternehmen verkauft Laborinstrumente für Gentests

bis hin zu Sequenzier- und DNA-Datenabgleichs-Geräten.

Der chinesische Markt für Gensequenzierung und ähnliche Technik für das Jahr 2017 wird auf 1 Mrd. US-Dollar geschätzt und soll sich in fünf Jahren verdoppelt haben. Thermo Fisher beschäftigt in China 5.000 Mitarbeitende und machte 2017 gemäß dem eigenen Geschäftsbericht 10% seiner Einnahmen in Höhe von insgesamt 20,9 Mrd. US-Dollar in diesem Land: „Unsere größte Erfolgsgeschichte in Neumärkten dauert in China an". Aus fünf Patentunterlagen des chinesischen Sicherheitsministeriums geht hervor, dass Ausrüstung von Thermo Fisher verwendet wurde, um die genetische Kartierung der Bevölkerung voranzubringen. Sicherheitsbehörden in Xinjiang bezogen Geräte von Thermo Fisher für „strafrechtliche Ermittlungen", wofür es in China noch keine technischen Alternativen gäbe. Gemäß den Patentunterlagen wurden ethnische Untersuchungen zu Uiguren, Tibetern und Han-Chinesen durchgeführt. Diese Differenzierungen seien für die Terrorbekämpfung nötig, „da entsprechende Fälle sonst schwerer zu knacken" seien.

Die Kooperation von Thermo Fisher wurde von dem republikanischen US-Senator Marco Rudio aus Florida und anderen kritisiert. Rubio forderte das US-Handelsministerium auf, Unternehmen den Verkauf von Technologie an China zu untersagen, die für Überwachungs- und Kontrollzwecke genutzt werden könne. Thermo Fisher kündigte daraufhin am 20.02.2019 an, „gemäß den Werten und den Ethik-Grundsätzen von Thermo Fisher" den Verkauf nach Xingjiang zu stoppen. Ein Firmensprecher sagte, als „weltweit führender Partner der Wissenschaft" müsse sich das Unternehmen damit befassen, „wie unsere Produkte und Dienstleistungen von unseren Kunden genutzt werden oder genutzt werden könnten".

Sophie Richardson, zuständig für China bei Human Rights Watch, begrüßte den Schritt von Thermo Fisher und erklärte, es müsse besser überprüft und überwacht werden, ob und wie nach China fließendes Know-how nach Xinjiang weitergegeben wird. Tahir Hamut, ein in Virginia lebender Filmmacher und Uigure, erklärte, es sei unvorstellbar, dass die Menschen angesichts der gegen sein Volk praktizierten Sanktionen ihr Blut freiwillig zu Verfügung stellten. Er selbst war im Mai 2017 von der Polizei in Xinjiang verhaftet worden; es wurden zwangsweise Blutproben, Fingerabdrücke, ein Gesichts- und Stimmscan erhoben. Einen Monat später sei er in einer örtlichen Klinik zur Durchführung eines freiwilligen Gesundheitschecks gewesen. Er habe 20 bis 40 verängstigte UigurInnen in einem Spalier stehen sehen: „Ohne eine solche Unterdrückung und ohne eine entsprechende persönliche Gefahr würde keiner seine Blutprobe für Forschungszwecke bereitstellen" (US-Firma verkauft keine Geräte mehr an China für DNA-Datenbank der Uiguren, www.zeit.de 22.02.2019; Sui-Lee, China Uses DNA to Track Its People, With the Help of American Expertise, www.nytimes.com 21.02.2019; vgl. DANA 2018, 53).

Brasilien

Gesichtserkennung im Karneval

In den Straßen von Rio de Janeiro feiern Hunderttausende Menschen Karneval, z. B. bei den großen Paraden im „Sambodrom" oder bei den Hunderten Straßenpartys und Umzügen, die in der ganzen Stadt stattfinden. Zum ersten Mal wurden im Jahr 2019 Kameras mit Gesichtserkennung eingesetzt, um die Menschenmassen zu kontrollieren. In Rios Stadtteil Copacabana werden die Aufnahmen der vorhandenen Verkehrskameras verwendet. In Salvador da Bahia, im Nordosten des Landes, wurden Kameras aufgebaut, die schon mit der Software zur Gesichtserkennung ausgerüstet sind. Oberst Anselm Brandao, der Polizeichef des Bundesstaats Bahia, begründete dies wie folgt: „Sicherheit geht vor. Das Besondere an diesem Karneval sind die neuen Technologien. Wir haben Kameras mit Gesichtserkennung. Aber auch Drohnen kommen zum Einsatz. Und an allen Zugängen stehen Spürhunde bereit."

Das neue System blieb bis Aschermittwoch in Betrieb. Die Gesichtserkennung soll, so die offizielle Begründung, dazu dienen, Straftäter, nach denen gefahndet wird, zu identifizieren. In Rio wird dazu das Facewatch-System verwendet, das auch in Großbritannien schon im Einsatz ist. Im System wurden die Gesichter von 1.100 gesuchten Straftätern hinterlegt. Der Computer soll Alarm schlagen, wenn sich einer von ihnen in Copacabana unter die Feiernden mischt. In Salvador da Bahia wird eine Software eingesetzt, die auch Behörden in China nutzen. Dort werden bekanntlich auch kleinere Vergehen wie Müll-Wegwerfen oder die Missachtung roter Ampeln verfolgt.

Die Behörden hoffen, dass die Software sogar noch hinter die Masken schauen kann und sich von Verkleidung nicht täuschen lässt. Matteus Torres, Techniker im Polizei-Einsatzzentrum von Rio, erläuterte: „Selbst, wenn die Person sich sehr verändert, zum Beispiel an Gewicht zunimmt oder abnimmt, bleibt die Position der Augen die gleiche. Und der wichtigste Faktor für eine hochwertige Gesichtserkennung ist nun einmal der Abstand zwischen den Augen." Datenschutz-Bedenken gibt es in Südamerika generell wenig. Kameraüberwachung ist weit verbreitet, z. B. in brasilianischen Einkaufszentren oder Flughäfen. Neu ist, dass sie umfassend im Freien und im Karneval verwendet werden (Marusczyk, Karneval in Brasilien, Die Gesichtserkennung feiert mit, www.tagesschau.de 01.03.2019).

Südkorea

Minikameras in Hotel-Föhns

Die Polizei hat zwei Männer verhaftet, die heimlich 1.600 Hotelgäste gefilmt und die Aufnahmen live online gestreamt haben sollen. Diese und zwei weitere Verdächtige sollen zwischen November 2018 und März 2019 in insgesamt 42 Zimmern in 30 Hotels Kameras installiert haben. Betroffen waren Hotels in zehn Provinzstädten des Landes. Die beiden Komplizen blieben auf freiem Fuß. Sie sollen den Tätern geholfen haben, die winzigen Kameras in der Halterung z. B. von Haarföhnen und Fernsehern zu integrieren. Die Polizei hat offenbar keine Hinweise darauf, dass die Hotels wussten, dass ihre Gäste ohne ihr Wissen gefilmt wurden. Die Kameras waren gemäß Presseberichten mit nur

etwa einen Millimeter großen Linsen im Badezimmer-Föhn oder einer Steckdosenabdeckung versteckt. Die Aufnahmen wurden demnach live an zahlende Kunden ins Internet gestreamt. Die Seite habe 4.099 Nutzende gehabt. 97 von ihnen hätten zudem etwa 45 Dollar für Extras wie Wiederholungen bezahlt. Insgesamt sollen die Täter mit den Aufnahmen mehr als 6.000 Dollar eingenommen haben.

Der Skandal um die heimlichen Videos erschüttert Südkorea nur Tage, nachdem der K-Pop Sänger Seungri nach Zuhälter-Vorwürfen seine Karriere vorläufig beendet hatte. Der 28-jährige soll auch Teil eines Chats gewesen sein, in dem heimlich gefilmte Sexvideos geteilt wurden. Verhaftet wurde außerdem der 30-jährige Sänger und Filmschauspieler Jung Joon-young. Auch dieser hatte sich beim Sex mit zehn verschiedenen Frauen heimlich gefilmt und diese Videos dann in einem Chat-Room mit Freunden geteilt. Die illegale Verbreitung von mit versteckten Kameras aufgenommenen Videos – Molka – ist in Südkorea ein ernst zu nehmendes soziales Problem. Weit verbreitet ist die Installation von Minikameras mit Sendern in öffentlichen Toiletten. Im Sommer 2018 erwischte die Polizei einen 13-Jährigen. Tausende Frauen hatten sich im vergangenen Jahr mehrmals zu Kundgebungen getroffen – und forderten stärkere staatliche Maßnahmen gegen die Verbreitung solcher Videos. Illegales Verbreiten von Videos wird in Südkorea mit bis zu fünf Jahren Gefängnis und bis zu 30 Mio. Won (ca. 23.000 €) Bußgeld geahndet. Dazu könnte eine Strafe wegen Verbreitung von Pornografie kommen. Seit 2013 sind mehr als 30.000 Fälle angezeigt worden. Zur Bestrafung kam es bisher selten. Die Polizei hat eigens eine Molka-Einheit geschaffen, die solche Kameras mit Funk- und Infrarot-Detektoren aufspüren kann.

Südkorea ist das am besten vernetzte Land der Welt mit dem schnellsten Internet, 94% der Bevölkerung haben ein Smartphone. KritikerInnen werfen der Industrie und der Regierung vor, sie würden die SüdkoreanerInnen als Versuchskaninchen benutzen. Sie lieferten ihnen ständig billige neue Technologien, auf welche die Gesellschaft nicht vorbereitet sei. Die Zahl junger Leute, die Games- oder Smartphone-süchtig sind, ist hier besonders groß. In den Schulen kommt es oft zu Belästigungen über die sozialen Medien (1600 Hotelgäste in Südkorea heimlich gefilmt, www.spiegel.de 21.03.2019; Neidhardt, Mini-Kameras im Föhn versteckt, SZ 22.03.2019, 10).

Technik-Nachrichten

Premium-Staubsauger vermessen die Wohnung

Das AV-Test-Institut hat vier Premium-Modelle von Staubsauger-Robotern untersucht und rät InteressentInnen vor einem Kauf die Datenschutzerklärungen zu den Produkten samt Steuerungs-App genau zu studieren. Oberklasse-Saugroboter sind zur Kommunikation mit den Hersteller-Servern und anderen Diensten ständig online und damit ein potenzielles Risiko für Datenschutz und Privatsphäre. Anders als günstigere Modelle, die nur mit Berührungssensoren ausgestattet sind und einfach bei Kollisionen ihre Fahrtrichtung ändern, erstellen Saugroboter aus dem Premium-Segment zur Navigation Karten der Wohnräume samt Hindernissen, teils sogar mit Fenstern und Türen. Die Lagedaten stammen von den Ultraschall-, Infrarot- und Lasersensoren sowie Kameras in den Robotern.

Die Daten und Karten kann die Robo-BesitzerIn in der Einrichtungs- und Steuerungs-App einsehen. Sie wandern vom Smartphone übers Internet aber auch auf die Server der Hersteller oder an eventuell verbundene Dienste. Da es sich dabei um schutzwürdige Informationen handelt, die durch Aktivität oder Inaktivität des Gerätes zudem verraten, ob jemand gerade daheim ist oder nicht, lässt sich den TesterInnen zufolge daraus zumindest eine grundsätzliche Missbrauchsgefahr ableiten (Wenn der Saugroboter zum putzenden Spion wird, rp-online.de 31.01.2019).

Stiftung Warentest warnt vor Ausforschung durch Sprachassistenten

Wer Sprachassistenten nutzt, gibt gemäß einer Untersuchung der Stiftung Warentest eine Menge von sich preis ohne überprüfen zu können, was mit den Daten passiert. Vernetzte Lautsprecher sollen mit ihren Sprachassistenten den Alltag erleichtern, doch sei dies mit erheblichen Datenschutzmängeln verbunden: In dem Vergleich der Stiftung Warentest kam keines der 18 untersuchten Geräte über die Note „befriedigend“ hinaus.

Auf den Lautsprechern laufen Amazons Sprach-Software Alexa, Google Assistent oder Siri von Apple. Wer einen solchen Dienst intensiv nutze, gebe „einen gehörigen Teil seiner Privatsphäre auf“. Die Nutzenden könnten aus den Datenschutzerklärungen nicht schlau werden. Dort sei nicht zu erkennen, was mit den persönlichen Informationen geschieht. Die Erklärungen seien viel zu lang, oft unklar formuliert und verschwiegen relevante Rechte der Nutzenden. Grundlegende Prinzipien des europäischen Datenschutzrechts würden nicht angemessen umgesetzt. Das sorgt für reihenweise Abwertungen in den Noten. Wem Privatsphäre und Datenschutz wichtig sei, der solle lieber die Finger von den digitalen Helfern lassen. Wer diese Kriterien für weniger wichtig erachte, erhalte einige Geräte mit guter Sprachbedienung und ordentlichem Klang.

Bei den Lautsprechern mit Alexa schnitten die beiden von Amazon selbst

produzierten Boxen Echo Plus (Note 3,1; rund 150 Euro) und Echo (3,2; 100 Euro) am besten ab. An dritter Stelle landete das Modell One von Sonos (3,3; 205 Euro). Unter den Boxen, die mit Google Assistent laufen, haben der JBL Link 20 (172 Euro) und der Onkyo Smart Speaker G3 VC-GX30 (86 Euro) mit der Note 3,4 das beste Ergebnis erzielt. Apples Homepod mit Siri (330 Euro) wurde mit 3,7 benotet (Stiftung Warentest kritisiert Vernetzte Lautsprecher gefährden die Privatsphäre, www.saarbruecker-zeitung.de 01.04.2019.

Rechtsprechung

EuGH

Deutsche Steuer-ID-Regelungen sind EU-rechtskonform

Gemäß einem Urteil des Europäischen Gerichtshofs (EuGH) vom 16.01.2019 verstößt die Abfrage der persönlichen Steuer-ID im Rahmen der Neubewertung zollrechtlicher Bewilligungen grundsätzlich nicht gegen EU-Recht (C-496/17). Allerdings beschränkt der EuGH den abgefragten Personenkreis auf Unternehmensverantwortliche und Personen, die für Zollangelegenheiten zuständig sind.

Das Finanzgericht Düsseldorf (FG) hatte den EuGH in einem Vorabentscheidungsverfahren nach der Zulässigkeit der Abfrage der Steuer-ID im Rahmen der Neubewertung zollrechtlicher Bewilligungen gefragt (4 K 1404/17). Das FG wollte wissen, ob die private Steuer-ID betroffener natürlicher Personen für die Entscheidung über die unternehmensbezogene Bewilligung abgefragt werden darf. Zum anderen bezweifelt es die Erforderlichkeit des weit gefassten Personenkreises, dessen Daten abgefragt werden sollen.

Der EuGH urteilte, dass die Abfrage der Steuer-ID im Rahmen der Neubewertung zollrechtlicher Bewilligungen mit dem EU-Recht vereinbar ist. Es hält die Abfrage der privaten Steuer-ID betroffener natürlicher Personen für rechtens, da die Daten für eindeutige Zwecke erhoben und verarbeitet werden. Die Maßnahme sei angemessen und erheblich, um den Zollbehörden die Prüfung zu ermöglichen, ob von der betroffenen Person ein wesentlicher steuer- oder zollrechtlicher Verstoß begangen wurde. Die Abfrage sei auf das notwendige Maß beschränkt, da Informationen über die weitere persönliche Situation – z. B. den Familienstand, die Religionszugehörigkeit oder die Einkünfte – gerade nicht Teil der Abfrage sind.

Der EuGH sieht auch keinen Verstoß in der Tatsache, dass private Daten für die Bewertung unternehmensbezogener Zwecke erhoben werden. Es sei gerechtfertigt, dass die Zollbehörden die Möglichkeit erhalten zu prüfen, ob die natürlichen Personen ihrerseits schwerwiegende Verstöße gegen steuer- oder zollrechtliche Vorschriften begangen haben. Dies gelte unabhängig davon, ob diese Verstöße im Rahmen der Wirtschaftstätigkeit des Unternehmens begangen wurden oder nicht.

Art. 24 Abs. 1 Unterabs. 2 des Implementierenden Rechtsakts zum UZK (UZK-IA) erfasst jedoch nicht weitere Personen als die, die für das Unternehmen verantwortlich sind, die Kontrolle über seine Leitung ausüben oder für seine Zollangelegenheiten zuständig sind. Nicht betroffen sind also die Mitglieder von Beiräten und des Aufsichtsrates, sowie Abteilungsleiter (sofern nicht mit Zollangelegenheiten befasst), die Leiter der Buchhaltung und die Zollsachbearbeiter. Geschäftsführende Direktoren werden erfasst, wenn sie für das Unternehmen verantwortlich sind oder die Kontrolle über seine Leitung ausüben. Der EuGH folgte weitestgehend der Linie des Generalanwaltes.

Das FG Düsseldorf wird bei der Fortsetzung des Verfahrens die Vereinbarkeit der Abfrage der Steuer-ID mit deutschem Recht zu prüfen haben. Nach der Rechtsprechung des Bundesfinanzhofs entspringt die Steuer-ID dem persönlichen Steuerverhältnis zwischen Bürger und Staat. Nicht eindeutig ist, ob das nationale Steuerrecht die Verwertung der Steuer-ID für unternehmensbezogene, zollrechtliche Zwecke erlaubt (Steuer-ID: EuGH billigt die Abfrage der Steuer-ID im Rahmen der Neubewertung von Bewilligungen, www.hza-seminare.de 18.01.2019).

BVerfG

Kfz-Kennzeichen-Scanning-Regelungen in Bayern, BaWü und Hessen verfassungswidrig

Gemäß zwei Beschlüssen des Bundesverfassungsgerichts vom 18.12.2018 sind die polizeirechtlichen Regelungen zum automatischen Scannen von Kfz-Kennzeichen in Bayern, Baden-Württemberg (BaWü) und Hessen wegen Verstoß gegen das Recht auf informationelle Selbstbestimmung teilweise verfassungswidrig (1 BvR 142/15 sowie 1 BvR 2795/09, 1 BvR 3187/10). Kennzeichenabgleiche sind danach zur Gefahrenabwehr und auch für die sogenannte Schleierfahndung prinzipiell erlaubt, doch müssen rechtliche Grenzen beachtet werden.

Geklagt hatten betroffene Autofahrer. Anlass sind die umstrittenen Polizeigesetze in den Bundesländern, die der Polizei erlauben, Kennzeichen automatisiert zu kontrollieren. Dabei wird das Nummernschild eines vorbeifahrenden Autos verdeckt erfasst, kurzzeitig gemeinsam mit Angaben zu Ort, Datum, Uhrzeit und Fahrtrichtung gespeichert und mit Kennzeichen abgeglichen, die in Fahndungsaufrufen enthalten sind. Ergibt der automatisierte Abgleich keinen Treffer, werden die Daten wieder gelöscht. Die Länder setzen das System zu unterschiedlichen Zwecken ein, zum Beispiel um Einbruchserien zu ermitteln oder Großveranstaltungen zu schützen.

Dabei gibt das BVerfG seine alte Rechtsprechung auf, wonach kein Ein-

griff vorliegt, wenn bei einer Kfz-Erfassung der Abgleich zu einem Nichttreffer führt und die Daten sogleich gelöscht werden: „In solchen Kontrollen liegen Grundrechtseingriffe gegenüber allen Personen, deren Kraftfahrzeugkennzeichen erfasst und abgeglichen werden, unabhängig davon, ob die Kontrolle zu einem Treffer führt." Für die Kennzeichenkontrollen müsse es einen hinreichend gewichtigen Anlass geben, damit der Grundsatz der Verhältnismäßigkeit gewahrt wird. Dem genügen die Vorschriften in Bayern nicht, da die Kontrollen nicht darauf beschränkt sind, Rechtsgüter von erheblichem Gewicht zu schützen. In Bayern hat der Freistaat keine Gesetzeskompetenz, um die Kontrollen – wie dort vorgesehen – unmittelbar zum Grenzschutz zu erlauben.

Die Regelungen in Baden-Württemberg und Hessen genügen ebenfalls nicht in jeder Hinsicht dem Verhältnismäßigkeitsgrundsatz. In beiden Ländern werden Kennzeichenkontrollen nicht umfassend auf den Schutz von Rechtsgütern von erheblichem Gewicht begrenzt und Kennzeichenkontrollen als Mittel der Schleierfahndung ohne eine ausreichend klare grenzbezogene Beschränkung erlaubt.

Soweit Baden-Württemberg automatisierte Kennzeichenkontrollen erlaubt, um polizeiliche Kontrollstellen und Kontrollbereiche zu unterstützen, mit denen nach Straftätern gefahndet wird, fehle es dem Land schon zur Einrichtung dieser Kontrollstellen an der Gesetzgebungskompetenz, da der Bund diese Kompetenz für den Bereich der Strafverfolgung wahrgenommen hat. Insofern ist die Kennzeichenkontrolle auch formell verfassungswidrig. Aus ebenfalls formellen Gründen sind auch die hessischen Regelungen zum Kfz-Scanning an polizeilichen Kontrollstellen verfassungswidrig, die zur Verhütung versammlungsrechtlicher Straftaten eingerichtet sind, ebenso wie die Regelung zur Einrichtung dieser Kontrollstellen selbst.

Die Vorschriften zum Abgleich der erfassten Kennzeichen müssen gemäß dem BVerfG in allen drei betroffenen Ländern verfassungskonform einschränkend so ausgelegt werden, dass jeweils nur die Fahndungsbestände zum Abgleich herangezogen werden dürfen, die zur Abwehr der Gefahr geeignet sind, die Anlass der jeweiligen Kennzeichenkontrolle ist. Das Gericht hat die verfassungswidrigen Vorschriften größtenteils übergangsweise für weiter anwendbar erklärt, und zwar bis zum 31.12.2019. Auch andere Bundesländer haben den Kennzeichenabgleich in ihren Polizeigesetzen vorgesehen. Weitere Klagen gegen Polizeiaufgabengesetze sind noch anhängig.

Der Klägervertreter in beiden Verfahren, Rechtsanwalt Udo Kauß, erläuterte: „Das Bundesverfassungsgericht hat anlasslosen Kontrollen eine Absage erteilt und die Zulässigkeit solcher Massenkontrollen vom Vorliegen einer konkreten Gefahrensituation abhängig gemacht. Auch dürfen nicht mehr pauschal polizeiliche Dateien für den Abgleich mit den eine Kontrollstelle passierenden Fahrzeugen eingesetzt werden. Ein großer Sieg für Bürgerrechte!" Der bayerische Informatiker und Beschwerde einlegende Kläger Benjamin Erhart meinte: „Wenn das Bundesverfassungsgericht beinahe schon regelmäßig Gesetze kippen muss, weil sie nicht verfassungsgemäß sind, bedeutet das, unsere Politiker machen ihre Arbeit nicht so gut, wie sie sein müsste. Statt Populismus wäre mehr Nachdenken angebracht. Statt nutzlosem Sicherheitstheater, das Geld in die Kassen einiger weniger IT-Firmen spült, sollte das Geld lieber in gute Ausbildung, Ausstattung und ausreichend Personal bei den Sicherheitsbehörden gesteckt werden."

Ein Sprecher des bayerischen Innenministeriums sagte, dass möglicherweise die Anlagen an grenznahen Orten abgebaut werden müssen. Außerdem werde überprüft, welche Straftatbestände für die Schleierfahndung genutzt werden. Dazu gehört es, die Entscheidungsgrundlagen für konkrete Kontrollen zu dokumentieren. Grundsätzlich sehe das Ministerium jedoch keinen Grund, seine bisherige Fahndungspraxis wesentlich zu ändern, für die auf Daten der Inpol-Datenbank zugegriffen wird.

Hessen und Baden-Württemberg nutzen bisher für den Datenabgleich die Sachfahndungsdaten des Schengener-Informationssystems, womit zunächst nicht nach dem Zweck der Kennzeichenkontrolle unterschieden wird. Das Gericht verlangt, dass der Datenabgleich auf die Fahndungsbestände beschränkt wird, die für die Kontrolle bedeutsam sind. Die Länder müssen also eine andere, spezifischere Datenbasis für die Schleierfahndung nutzen. Die Innenministerien von Hessen und Baden-Württemberg hatten sich zunächst nicht zu dem Urteil geäußert.

Kontrovers diskutiert wurde nach den Beschlüssen, inwieweit dadurch die automatisierte Kontrolle der Einhaltung von Dieselfahrverboten mit Hilfe von Kfz-Kennzeichen-Scanning möglich bleibt, wie sie von Bundesverkehrsminister Andreas Scheuer (CSU) geplant ist. Der baden-württembergische Landesdatenschützer Stefan Brink meinte, dass diese nach wie vor im Bereich des Möglichen sei, da die Überwachung räumlich begrenzt stattfindet und für einen grundrechtlich hoch bewerteten Zweck unternommen wird. Das Gericht hält anlasslose Kontrollen für möglich, wenn sie an der „besonderen Verantwortung der Betroffenen für die Allgemeinheit" anknüpfen. Der Bürgerrechtlicher Patrick Breyer, einer der Kläger, hingegen glaubt, dass die Fahrverbots-Scanner-Pläne vom Tisch seien, weil sie nicht dem Schutz von Rechtsgütern von erheblichem Gewicht dienen.

Brink bedauert es, dass die Karlsruher Richter keine klaren Kriterien aufgestellt haben, anhand derer sich die Rechtmäßigkeit eines solchen Einsatzes rasch klären lasse. Stattdessen führe die am Verfassungsgericht weit verbreitete „Abwägeritis" dazu, in immer feineren argumentativen Verästelungen Möglichkeitsräume zu eröffnen. Die Politik neige dann dazu, diese Räume bis auf das Maximale auszunutzen. Anstatt also einer datenschutzfreundlichen „Blauen Plakette" bei den Dieselfahrverboten den Vorzug zu geben, setze sie lieber auf die grundrechtsinvasivere Kennzeichenerfassung.

Die Erfassung von Kennzeichen für die Abrechnung der Maut auf Autobahnen wird nach Ansicht der niedersächsischen Aufsichtsbehörde der Landesbeauftragten für den Datenschutz Barbara Thiel durch die Beschlüsse des BVerfG nicht direkt tangiert. Auch für Blitzer-Anlagen darf sie noch verwendet werden. Dabei werde nämlich nur der Fahrer erfasst, der bei der Geschwindigkeitsübertretung unmittelbar in flagranti

erwischt wird. Anders ist das jedoch bei neuen Geschwindigkeitsmesssystemen, die unterschiedslos alle Fahrzeuge erfassen, dem Section-Control-Verfahren. Gemäß dem Stellvertreter von Thiel, Christoph Lahmann, müsse dieses Verfahren nun eingestellt werden, das an der B6 bei Laatzen im Dezember 2018 in Betrieb genommen wurde und bei dem seit Januar 2019 für Geschwindigkeitsübertretungen Bußgelder erhoben werden. Ändern würde sich die Rechtslage erst wieder, wenn das geplante neue Polizeirecht in Niedersachsen in Kraft träte, das eine gesetzliche Grundlage für Section Control vorsieht (dazu siehe unten VG Hannover; Wilkens, Kfz-Kennzeichen-Scanning teilweise verfassungswidrig, www.heise.de 05.02.2019; Kurzlink: https://heise.de/-4297821; Autokennzeichen-Abgleich zum Teil verfassungswidrig, www.sueddeutsche,de 05.02.2019; PE HU 05.02.2019, Bundesverfassungsgerichtsurteil zur Kfz-Kennzeichenkontrolle: Ein großer Sieg für die Bürgerrechte!; Schulzki-Haddouti, Kfz-Kennzeichen-Scanning auf dem Prüfstand, www.heise.de 06.02.2019, Kurzlink: https://heise.de/-4299849; Wilkens, Section Control: Datenschutzbeauftragte fordert sofortigen Streckenradar-Stopp, www.heise.de 06.02.2019, Kurzlink: https://heise.de/-4299763).

VG Hannover

Probebetrieb „Section Control“ fehlt gesetzliche Grundlage

Das Verwaltungsgericht Hannover (VG) hat am 12.03.2019 dem Antrag auf Erlass einer einstweiligen Anordnung sowie einer Klage stattgegeben, mit denen der Antragsteller und Kläger begehrte, dass das Land Niedersachsen es unterlässt, Geschwindigkeitskontrollen hinsichtlich der von ihm geführten Fahrzeuge mittels der Anlage „Section Control“ auf der B6 in Laatzen zwischen den Anschlussstellen Gleidingen und Laatzen durchzuführen (Klage: 7 A 849/19, Eilverfahren: 7 B 850/19). Durch „Section Control“ werden die Kfz-Kennzeichen aller in dem überwachten Abschnitt einfahrenden Fahrzeuge erfasst. Auch wenn diese beim 2,2 km entfernten Ausfahren im sog. Nichttrefferfall gelöscht werden, bedarf es, so das VG, für deren Erfassung – sowohl im sog. Treffer- als auch im sog. Nichttrefferfall – einer gesetzlichen Ermächtigungsgrundlage, da in das verfassungsrechtlich garantierte informationelle Selbstbestimmungsrecht eingegriffen wird. Für einen solchen Eingriff bedarf es stets – auch ungeachtet der jeweiligen Schwere des Eingriffs – einer gesetzlichen Grundlage. Dass „Section Control“ sich noch im Probebetrieb befindet, ändere hieran nichts. Das VG bezog sich dabei auch auf den jüngsten Beschluss des Bundesverfassungsgerichts vom 18.12.2018 zur automatisierten Kraftfahrzeugkennzeichenkontrolle zum Abgleich mit dem Fahndungsbestand (1 BvR 142/15 u. 1 BvR 2795/09, 1 BvR 3187/10; s. o.).

An einer solchen gesetzlichen Grundlage fehlt es hier. Dies zeigt sich nicht zuletzt darin, dass im Niedersächsischen Landtag ein entsprechender Gesetzentwurf zur Änderung des Niedersächsischen Polizeirechts (LT-Drs. 18/850) eingebracht ist, in dem mit § 32 Abs. 8 NPOG-E eine Rechtsgrundlage geschaffen werden soll. Die 7. Kammer des VG ließ es dahingestellt, ob eine solche Rechtsgrundlage in die Gesetzgebungskompetenz des Landes Niedersachsen fällt oder der Bundesgesetzgeber tätig werden müsste. Zum Zeitpunkt der Entscheidungen existierte weder auf Bundes- noch auf Landesgesetzesebene eine Ermächtigungsgrundlage.

Der Antragsteller und Kläger muss einen Eingriff in seine Rechte auch nicht während eines Probebetriebes hinnehmen. Aus dem Rechtsstaatsprinzip und dem Gewaltenteilungsgrundsatz folge, dass die Exekutive nicht selbst so handeln darf, als hätte der Gesetzgeber sie hierzu schon ermächtigt. Der Staat sei auch nicht zwingend auf „Section Control“ angewiesen. Er kann die Verkehrsüberwachung bis zur Schaffung einer Rechtsgrundlage auch auf andere Weise durchführen. Gegen die Entscheidungen kann das Land Niedersachsen Rechtsmittel einlegen (PE VG Hannover 12.03.2019, Keine gesetzliche Grundlage für Verkehrsüberwachung mittels „Section Control“ – 7. Kammer gibt Eilantrag und Klage statt).

KG Berlin

Google-AGB umfassend unzulässig

Gemäß einem Urteil des Kammergerichts Berlin (KG) vom 21.03.2019 enthielt die Google-Datenschutzerklärung von 2012 viele rechtswidrige Klauseln (Az. 23 U 268/13). Geklagt hatte der Verbraucherzentrale Bundesverband (vzbv). In den Allgemeinen Geschäftsbedingungen (AGB) hatte Google sich umfangreiche Rechte zur Erhebung und Nutzung von Kundendaten eingeräumt. Beispielsweise wollte Google personenbezogene Daten aus den verschiedenen Diensten miteinander verknüpfen oder in bestimmten Fällen an Dritte weitergeben. Der vzbv stellte fest: „Einige der untersagten Klauseln verwendet Google bis heute in gleicher oder ähnlicher Form.“

Das Gericht sieht einen Verstoß gegen die Datenschutz-Grundverordnung (DSGVO) darin, dass die Datenschutzerklärung den Eindruck erweckt, dass die beschriebene Datenverarbeitung ohne Zustimmung der KundInnen erlaubt sei, während tatsächlich für die Nutzung von personenbezogenen Daten die „informierte und freiwillige Einwilligung“ der Anwendenden erforderlich ist. Es reiche nicht aus, dass die VerbraucherInnen die Datenschutzerklärung (oft ungelesen) abnicken. Heiko Dünkel, Rechtsreferent beim vzbv: „Es wird höchste Zeit, dass Google Verbraucherrechte und Datenschutz endlich ernst nimmt und seine Bedingungen fair und transparent gestaltet“.

Das KG sah Teile von Googles Datenschutzerläuterungen zudem als unwirksam an, weil sie „so verschachtelt und redundant ausgestaltet“ seien, dass die Nutzenden sie kaum hätten durchschauen können. Insgesamt erklärte das Gericht 13 Klauseln in der Datenschutzerklärung für unwirksam. Google schreibt darin etwa, einzelne Dienste nach eigenem Ermessen einzustellen oder zu ändern. Das ist nach Ansicht des KG ein gesetzlich nicht zulässiger Änderungsvorbehalt. Google dürfe die versprochenen Leistungen nur dann ändern, wenn das für seine KundInnen auch zumutbar sei. Die Klausel enthielt jedoch keine solche Einschränkung. Google ist bekannt

dafür, Dienste rigoros einzustellen, die nicht mehr in die Strategie passen.

Das Gericht gab der Klage des vzbv in vollem Umfang statt. In erster Instanz hatte bereits das Landgericht Berlin so entschieden. Das jetzige Urteil ist noch nicht rechtskräftig. Google hat laut vzbv eine Nichtzulassungsbeschwerde beim Bundesgerichtshof eingelegt (Berger, Urteil: Google-Datenschutzerklärung verstieß gegen DSGVO, www.heise.de 16.04.2019, Kurzlink: https://heise.de/-4400575).

KG Berlin

Apple-AGB weitgehend unzulässig

Das Kammergericht Berlin (KG) hat mit Urteil vom 27.12.2018 das Urteil des Landgerichts Berlin (LG) vom 30.04.2013 (15 O 92/12, DANA 2013, 79 ff.) weitgehend bestätigt, wonach Apple zentrale Datenschutzklauseln nicht mehr verwenden darf (Az.: 23 U 196/13). Geklagt hatte der Verbraucherzentrale Bundesverband (vzbv) gegen die Apple Sales International, die damals in Deutschland den App Store der Kalifornier betrieb. Das KG erklärte eine „Richtlinie" des App-Store-Betreibers in weiten Teilen für rechtswidrig, mit der sich dieser weitgehende Rechte zur Nutzung von Kundendaten einräumte. Das Unternehmen wollte demnach sogar „präzise Standortdaten" der Anwender für Werbezwecke auswerten und persönliche Informationen an „strategische Partner" weitergeben. In der umstrittenen Erklärung auf den Apple-Seiten hieß es damals unter anderem: „Wenn Sie mit Apple oder einem mit Apple verbundenen Unternehmen in Kontakt treten, können Sie jederzeit dazu aufgefordert werden, personenbezogene Daten anzugeben. Apple und seine verbundenen Unternehmen können diese personenbezogenen Daten untereinander austauschen und sie nach Maßgabe dieser Datenschutzrichtlinie nutzen. Sie können solche Daten auch mit anderen Informationen verbinden, um unsere Produkte, Dienstleistungen, Inhalte und Werbung anzubieten oder zu verbessern."

Der Konzern nahm es sich auch heraus, personenbezogene Informationen zur Werbung oder für „interne Zwecke" zu verwenden. Sie sollten auch dazu dienen, um Produkte, Dienste oder Inhalte zu entwickeln oder zu verbessern. Das LG hatte diese Klauseln für unzulässig erklärt, da solche „globalen Einwilligungen" untersagt seien. Es bleibe unklar, welche Daten in welchem Umfang genutzt werden könnten. Das KG prüfte die Passagen angesichts der auch auf die Zukunft ausgerichteten Unterlassungsklage nun auch anhand der seit Mai 2018 geltenden Datenschutz-Grundverordnung (DSGVO).

Der Senat hält es für eindeutig, dass die „bloß einseitige Verlautbarung bestimmter Datenverarbeitungspraktiken" keine Einwilligung des Betroffenen darstelle. Die Klauseln vermittelten den VerbraucherInnen den unzutreffenden Eindruck, dass Apple die thematisierten personenbezogenen Daten verarbeiten dürfe, ohne dass es auf ein Opt-in der Nutzenden ankomme. Auch eine reine Unterrichtung der Anwendenden macht die ausgeübten Praktiken nicht rechtmäßig und nähre Fehlvorstellungen rund um die Frage der Einwilligung. Die Gefahr, dass der Konzern sein Handeln fortsetze oder wiederhole, bezeichnet die Berufungsinstanz als akut: Die Klauseln würden nämlich „jetzt von einer anderen Gesellschaft der Apple-Unternehmensgruppe" eingesetzt.

Aus dem Schneider wäre der Konzern erst, „wenn es zu einer endgültigen Geschäftsaufgabe kommt". Derzeit sei aber nicht auszuschließen, dass die Beklagte im Zuge einer erneuten Umstrukturierung auch wieder den Online-Store übernehme und wie die „jetzige Betreiberin die Datenschutzrichtlinie in ihrer früheren Fassung weiterverwendet". Der Store wird mittlerweile von einer anderen Apple-Tochter betrieben.

Durchgehen ließ das Kammergericht im Gegensatz zur Vorinstanz allein eine Klausel, wonach die Kalifornier Kontaktdaten Dritter wie Name, Adresse, E-Mail oder Telefonnummern erheben dürfen, wenn Nutzende Inhalte etwa mit der Familie oder Freunden teilen oder Geschenkgutscheine des Unternehmens verwenden. In diesen Fällen seien die Informationen tatsächlich zur Vertragserfüllung erforderlich. Die Revision hat das Berufungsgericht nicht zugelassen und das Urteil für vorläufig vollstreckbar erklärt. Laut dem vzbv ist der Beschluss aber noch nicht rechtskräftig, weil sich Apple mit einer Beschwerde dagegen zur Wehr setzt.

Apple gibt sich gern als Vorreiter beim Datenschutz aus. Das Urteil und der Umgang Apples damit lassen hieran jedoch zweifeln. Der Rechtsreferent des vzbv Heiko Dünkel begrüßte die Entscheidung: „Das Kammergericht hat klargestellt, dass auch ältere Klauseln zur Nutzung personenbezogener Daten die Anforderungen der seit Mai 2018 geltenden DSGVO erfüllen müssen." Er bedauerte, dass sich einige der Formulierungen so oder ähnlich immer noch in den aktuellen Datenschutzbestimmungen des Shops fänden (Krempl, Apple-Datenschutzrichtlinie ist größtenteils rechtswidrig, www.heise.de 22.02.2019; Kurzlink: https://heise.de/-4316486).

LG Düsseldorf

Kein strafrechtliches Verwertungsverbot von unzulässigen Bodycam-Aufnahmen

Das Landgericht (LG) Düsseldorf hat am 15.02.2019 entschieden, dass die Bodycam-Aufnahmen von Polizisten als Beweismittel in Prozessen herangezogen werden dürfen, auch wenn die Kamera gar nicht hätte aufnehmen sollen (1 Ks 19/18). Die Voraussetzungen für den Einsatz von Bodycams waren erst zwei Jahre zuvor in Nordrhein-Westfalen gesetzlich geregelt worden. Die neuen Körperkameras sollen dem Schutz der PolizistInnen dienen.

Im konkreten Fall ist eine 60-Jährige wegen Tötung ihres Ehemanns angeklagt. Eine Polizistin, die nach Eingang des Notrufs mit einem Kollegen zuerst die Wohnung der Eheleute betreten hatte, hatte dabei die Kamera eingeschaltet. Der Verteidiger der Angeklagten hatte argumentiert, die Beamtin hätte die Aufnahmen stoppen müssen, als sie am Ort des Geschehens festgestellt hatte, dass keine Gefahr bestand. Das sah auch das Gericht so. Es sei aber „lebensnah", dass die Beamtin in der Situation vergessen habe, die Kamera abzustellen. Ein Beweisverwertungsverbot ergebe

sich daraus dennoch nicht. Die Videoaufnahmen wurden nach Bekanntgabe des Beschlusses im Prozess gezeigt.

Notfalls werde der Bundesgerichtshof in der Revision über die Zulässigkeit der Aufnahmen als Beweismittel entscheiden müssen, sagte Verteidiger Nicolai Mameghani auf Anfrage. Er strebe einen Freispruch für seine Mandantin an. Mameghani hatte für die Angeklagte erklärt, dass es sich um einen Unfall gehandelt habe. Der Ehemann habe seiner Frau in der Küche auf die Schulter geschlagen. Er sei dabei selbst in Socken auf glattem Boden ausgerutscht und auf sie gestürzt. Weil sie gerade Brot schnitt, habe die Frau ein Messer in der Hand gehalten. Beide seien zu Boden gefallen. Das Messer habe sich in den Bauch des Ehemanns gebohrt. Er war verblutet.

Das Geschehene hatte sich am 20.05.2018 in Düsseldorf in der Wohnung des Ehepaars abgespielt. Das Paar soll zuvor einen Streit gehabt haben, weil er länger in einer Kneipe bleiben wollte und sie auf den Heimweg gedrängt habe. Die Polizistin soll die Kamera etwa eine halbe Stunde lang eingeschaltet gehabt haben. Das Verhalten der Angeklagten, die dabei gefilmt worden war, soll diese aus Sicht der Staatsanwaltschaft belasten (Gericht erklärt Bodycam-Aufnahmen für zulässiges Beweismittel, www.heise.de 16.02.2019, Kurzlink: https://heise.de/-4311087).

OLG Wien

Anforderungen an Wahrheitsbeweis bei Internet-Gegenwehr

Das Oberlandesgericht (OLG) Wien hob am 12.03.2019 ein Urteil des Landgerichts für Strafsachen (LG) Wien vom Oktober 2018 auf, in dem die 33-jährige Parlamentsabgeordnete (2013-2017) und Grünen-Politikerin Sigi Maurer zu einer Geldstrafe von 7.000 € plus Verfahrenskosten verurteilt worden ist, weil sie einen Screenshot einer erhaltenen privaten Facebook-Nachricht veröffentlicht hatte einschließlich Name und Geschäftsadresse des Absenders. Die Nachricht hatte folgenden Inhalt, nachdem sie Ende Mai 2018 in Wien an einem Getränkeladen vorbeigegangen war: „Hallo Du bist heute bei mir beim Geschäft vorbei gegangen und hast auf meinen Schwanz geguckt als wolltest du Ihn essen." In einer weiteren Nachricht ließ sich der Verfasser über Maurers Figur aus und beleidigte sie als „kleine dreckige Bitch !!!" Die obszönen Botschaften stammten vom Account des Besitzers eines Craftbeershops. Sie kommentierte: „Ich dachte mir, in einer Stadt voller Hipster schadet es ja nicht, darüber zu informieren, bei welchem frauenverachtenden Arschloch man potenziell sein (craft) Bier kauft". Wer wissen wolle, warum dieser Mann Frauen belästige, „kann ja mal bei ihm nachfragen." Der Geschäftsbesitzer wurde nach eigenen Angaben zufolge daraufhin beschimpft und mehrfach bedroht.

Maurer begründete ihr Vorgehen damit, dass derartige Zuschriften nach österreichischem Recht nicht strafbar seien. Beleidigungen setzen demnach Öffentlichkeit voraus. Sie habe sich nicht anders zu helfen gewusst, als die Botschaften und den Absender öffentlich zu machen. Der Besitzer des Ladens verklagte Maurer. Er habe die Nachrichten gar nicht geschrieben, der Computer stehe in seinem Geschäftsraum und sei auch für Kunden zugänglich. Er wisse nicht, wer Maurer angeschrieben habe. Er sei es jedenfalls nicht gewesen. Der Mann machte geltend, er fühle sich zu Unrecht an den Pranger gestellt und habe massive Beschimpfungen, Bedrohungen und wirtschaftlichen Schaden erlitten. Das LG folgte in weiten Teilen der Argumentation des Klägers und verurteilte Maurer wegen übler Nachrede zu einer Geldstrafe in Höhe von 3.000 € sowie zu einer Zahlung an den Kläger „wegen erlittener Unbill" in Höhe von 4.000 €.

Im ersten Prozess hatte das LG konstatiert, Maurer habe nicht nachweisen können, dass die beleidigenden Nachrichten tatsächlich von dem Ladenbesitzer verfasst worden seien. Der Richter erklärte: „Ich bin überzeugt, dass der Kläger lügt." Es sei aber nicht zweifelsfrei festzustellen gewesen, von wem die Nachricht stammte. Maurer hätte sich im Sinne der „journalistischen Sorgfaltspflicht" vor der Veröffentlichung der Nachrichten vergewissern müssen, dass der Text tatsächlich von der Person versendet worden ist, auf deren Namen das Profil lief. Maurer erfuhr nach dem Urteil aus der Bevölkerung breite Unterstützung. Ihre Spendenkampagne für einen „Rechtshilfefonds gegen Hass im Netz" sammelte binnen 38 Stunden 100.000 €. Der Bierhändler forderte daraufhin eine höhere Schadenssumme, da sie sich nach der Spendenaktion in anderer finanzieller Lage befände als zuvor.

Das Oberlandesgericht urteilte nun, es sei nicht ausreichend gewürdigt worden, „dass die Nachrichten immerhin vom Computer und vom Facebook-Account des Privatanklägers versendet wurden". Bei der „Beurteilung des Wahrheitsbeweises" sei „eine gewisse Lebensnähe zu beachten" Dies sei im ersten Prozess nicht geschehen: „Das Erstgericht hat die Latte für den Wahrheitsbeweis geradezu unerreichbar hoch angesetzt." Das bedeute, dass schon die bloße Behauptung ausreiche, auch andere Personen hätten Zugang zum Computer, um den Beweis unmöglich zu machen, „dass doch der Inhaber des Geräts die Mitteilungen versendet hat".

Der Kläger habe aber nicht schlüssig darstellen können, dass konkret eine andere Person die Nachricht geschrieben und versendet habe. Das Szenario eines anderen Verfassers sei „im konkreten Fall und wenn man die übrigen Beweisergebnisse berücksichtigt, eigentlich nicht vorstellbar". Der „unbekannte Verfasser" hätte wenig Zeit gehabt, dies unbemerkt zu tun; und er hätte gleichzeitig beobachten müssen, ob der Ladenbesitzer während des Verfassens der Nachricht ins Lokal zurückkommt. Im ersten Prozess hatten Zeugen ausgesagt, sie hätten im Ladenlokal niemanden gesehen, der zum Computer gegangen wäre. Der Prozess muss in erster Instanz wiederholt werden. Die Richter widersprachen der Einschätzung, Maurer sei der Wahrheitsbeweis nicht gelungen, dass wirklich der Bierladenbesitzer die Nachrichten versendet habe.

Maurer erklärte nach dem OLG-Urteil: „Ich fühle mich in meiner Wahrnehmung bestätigt, dass die Urteilsbegründung absurd war". Sie hofft auf einen Freispruch in der Wiederholung und auf eine Gesetzesänderung: „Noch habe ich nicht gewonnen" (Kazim, Üble Nachrede Gericht hebt Urteil gegen Ex-Politikerin Sigi Maurer auf, www.spiegel.de 12.03.2019; Al-Serori, Flaschenpost, SZ 13.03.2019 8).

Buchbesprechungen

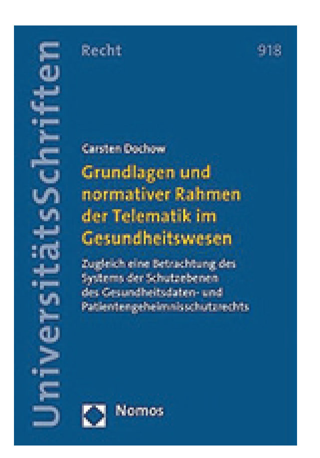


Gola, Peter/Heckmann, Dirk (Hrsg.)
Bundesdatenschutzgesetz – Kommentar
13. Aufl. 2019, C.H.Beck,
ISBN 978-3-406-72878-5, 792 S., 89,00 €.

(tw) Es ist nur auf den ersten Blick verwirrend, dass in Zeiten der DSGVO plötzlich eine Neuauflage eines Kommentars zum BDSG erscheint. Der Gola/Schomerus gehörte ja bis zur 12. Auflage zu den Standardkommentaren zum alten Bundesdatenschutzgesetz (BDSG a.F.), das seit dem 25.05.2018 nicht mehr in Kraft ist. Peter Gola machte aus dieser Not eine Tugend und zählt nun den völlig neuen Kommentar zum völlig neuen BDSG und mit neuer Mitherausgeberschaft auflagenmäßig einfach weiter. Der Kommentar beschränkt sich auf das neue BDSG, das nichts anderes tut, als die europäische DSGVO zu ergänzen, auszufüllen und teilweise aufzuheben. Für eine umfassende Kommentierung des allgemeinen Datenschutzrechts muss also zusätzlich auf ein Werk zur DSGVO zurückgegriffen werden, wovon es inzwischen ja viele gibt – auch ein von Gola herausgegebenes in 2. Auflage.

Wurde der alte Gola/Schomerus mit jeder neuen Auflage einfach ergänzt, so musste nun mit der Kommentierung von vorne begonnen werden, was bei den stattlichen 85 Paragraphen nicht mehr (wie die 12. Auflage) von drei Bearbeitenden bewerkstelligt werden konnte: 19 BearbeiterInnen weist das Werk auf. Und diese kümmern sich nicht nur um die §§ 1-44, also die Umsetzung der DSGVO, sondern auch um die darauf folgenden BDSG-Regelungen, die sich der bundesdeutschen Umsetzung der JI-Datenschutz-Richtlinie widmen, also der Richtlinie (EU) 2016/680 (JI-DSRl). Diese Regeln, also die §§ 45-85, sind von höchster Relevanz, alldieweil es um die Verarbeitung – vulgo – durch Polizei und Justiz, also für Zwecke der Gefahrenabwehr und der Strafverfolgung geht. Diese Regelungen sind weniger im öffentlichen Fokus, einmal als kleiner Bruder zur DSGVO, dann aber auch wegen ihrer Lückenbüserfunktion ergänzend z. B. zum Polizeirecht des Bundes. Und insofern finden diese Regelungen regelmäßig auch ihre Entsprechung in Landesregelungen – auch dort gemäß dem Bundesvorbild zumeist, aber nicht überall – in den Landesdatenschutzgesetzen. Die Antwort auf die Frage, welches Datenschutzrecht gilt, wird noch mehr als bisher zur Wissenschaft, weshalb wir auch Kommentierungen brauchen. Die Landesreferenzen werden im Gola/Heckmann jeweils aufgeführt.

Dass die in dem Werk gelieferten Antworten auf Auslegungsfragen die letzte Weisheit sind, behaupten die AutorInnen selbst nicht. Zu offen sind viele Auslegungsmöglichkeiten, zu wenig Rechtsprechung liegt bisher vor. Dieser Kommentar gibt erste Antworten, manchmal nur Hinweise. Diese Antworten tragen die Handschriften der jeweiligen AutorInnen, die sich teilweise stark unterscheiden. Aber fast durchgängig kann festgestellt werden, dass eine gediegene Literaturauswertung erfolgt ist. Man kann aber – wie bei den meisten neueren Datenschutzkommentaren – keine einheitliche Linie feststellen: weder besonders betroffenen- noch besonders verarbeitungsfreundlich. Das Werk ist dem Erklären der Regeln und deren Auslegung gewidmet, aber nur eingeschränkt einer kritischen Durchdringung. Die Verfassungs- und Grundrechtsbezüge gehen dabei ebenso unter wie ein allzu kritisches Messen des BDSG an seinen europäischen Vorgaben, der DSGVO und der JI-DSRl. Zwar wird erwähnt, dass manche Regelungen kritisiert wurden und werden – mit welchen Argumenten und mit welcher Berechtigung wäre aber auch erwähnenswert gewesen. Eine Vertiefung von eklatant verfassungs- und europarechtswidrigen Regeln wie die übermäßige Beschränkung der Betroffenenrechte oder der Kontrollausschluss bei Berufsgeheimnissen sollte spätestens in der 14. Auflage zu finden sein. So bleibt der Gola/Heckmann ein Anwendungskommentar mit vielen Hinweisen, Quellen und Erläuterungen. Er könnte insofern wieder zum Standardwerk werden. Doch allein darauf verlassen sollten sich grundrechtskritische DatenschützerInnen nicht.



Carsten Dochow
Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen
Zugleich eine Betrachtung des Systems der Schutzebenen des Gesundheitsdaten- und Patientengeheimnisschutzrechts
Nomos Baden-Baden,
ISBN 978-3-8487-4268-4, 1520 S., 189 €.

(tw) Die wissenschaftliche Bearbeitung des Gesundheitsdatenschutzes ließ lange Zeit viele Wünsche offen. Eine erste umfassende Begutachtung legten vor wenigen Jahren Kingreen/Kühling vor (DANA 2015, 106 f.). Diese kamen schon zu dem Ergebnis, dass das Regelungsregime in diesem Bereich eher chaotisch ist und aufgeräumt gehört.

Dies ist letztlich auch das Ergebnis der zweiten umfassenden Behandlung des Themas durch Dochow. Seine opulente Dissertation ist die bisher ausführlichste und detaillierteste Untersuchung des Gesundheitsdatenschutzes.

Zwar zielt Dochow letztlich auf die Gesundheitstelematik ab, also den digitalen Austausch von Gesundheitsdaten im Behandlungskontext, doch ist sein Werk umfassender angelegt und liefert eine Rundumdarstellung des Datenschutzes, dann des Gesundheitsdatenschutzes mit Standes- und Strafrecht, um dann ins Detail der §§ 291a SGB V einzusteigen mit der elektronischen Gesundheitskarte und den sog. eHealth-Anwendungen. Das Los von Promotionen zum Datenschutz während der Entstehungsphase der DSGVO ist, dass der Doktorand an lebenden Körper operieren musste, also an einer sich ändernden rechtlichen Landschaft. Dies gelingt Dochow, der zwar noch von der Anwendbarkeit des alten BDSG ausgeht, aber auch dessen völlige Überarbeitung 2017 sowie die DSGVO im Blick hat wie auch die grundlegende Ausweitung der Berufsgeheimnisses auf „Mitwirkende" in § 203 Abs. 3, 4 StGB.

Dochow kommentiert sowohl den bisherigen Rechtszustand als auch die Änderungen meinungsstark und kritisch. So sieht er im Standesrecht keine Befugnisgrundlagen für Eingriffe in Patientenrechte. Zu Recht kritisiert er die Uferlosigkeit der Öffnung des § 203 StGB und macht konstruktive Vorschläge für eine Einhegung. Er plädiert für ein einheitliches Gesundheitsdatenschutzrecht oder zumindest für ein Gesundheitstelematikgesetz, erkennt aber realistisch, dass dies angesichts der politischen Debatte wohl im Bereich des Wünschenswerten bleiben wird.

Das Buch ist eine wahre Fundgrube in Bezug auf das umfangreiche, aber völlig unübersichtliche Schrifttum zum Thema. Sein Literaturverzeichnis ist wohl das vollständigste, das mir zum Thema bekannt ist. Es ist auch eine Fundgrube für Ideen und Erwägungen, die er nicht nur aus dem Schrifttum zitiert, sondern oft selbständig entwickelt. Das Ganze ist in einer gefälligen Sprache formuliert, die einem das Verständnis der sperrigen Materie leichter macht.

Das Buch hätte etwas schlanker werden können, wenn auf die Grundlagen des Datenschutzes kürzer eingegangen worden wäre, die nun schon an vielen Stellen nachgelesen werden können. Dadurch, dass der Autor aber auch den internationalen Rechtsrahmen mitbehandelt, sind selbst die allgemeinen Ausführungen interessant. Der Hauptwert liegt aber in der dogmatischen Aufbereitung des Gesundheitsdatenschutzrechts mit seiner telematischen Spezifik – ein Thema, das uns noch Jahrzehnte beschäftigen wird. Durch die gründliche Aufbereitung liegt hier ein Fundament, auf das es aufzubauen gilt. Dafür ist/wäre die Politik gefordert. Diese wird aber sicher keine 1.300 Seiten studieren. Deshalb sind Übersetzungsleistungen wichtig, wozu der Autor bei seiner jetzigen Beschäftigung in der Bundesärztekammer die Gelegenheit hat.



Buchner, Benedikt (Hrsg.)
Datenschutz im Gesundheitswesen
AOK-Verlag Remagen, 2. Aufl. 2019
ISBN 978-3-553-43110-1, 384 S., 89,90 €

(tw) Die knapp ein Jahr alte erste Auflage ist offenbar vergriffen (vgl. DANA 2/2018, 122), weshalb der Verlag schon eine neue Auflage auf den Markt wirft – diesmal ohne „Der NEUE" im Titel. Dass dies nötig bzw. möglich ist, liegt anscheinend an dem starken Bedarf: Eine aktuelle Einführung in den nicht unkomplizierten Datenschutz im Gesundheitsbereich stößt bei PraktikerInnen weiterhin auf eine große Nachfrage. Grundlage auch der zweiten gebundenen Auflage ist die weitergeführte Loseblattausgabe (DANA 3/2017, 181), die in der Struktur beibehalten wird, aber in Bezug auf Gesetzgebung auf Bundes- und Landesebene und Literatur und ein wenig Rechtsprechung aktualisiert wurde. Wer die erste Auflage hat, benötigt also nicht zwingend die zweite.

Zugleich wird das Werk weiter konsolidiert: Die Autoren Sebastian Ertel, Dennis-Kenji Kipker, Lutz-Udo Pampel und Sven Venzke-Caprarese sind allesamt Praktiker, die gemeinsam mit den Herausgebern die Grundlagen des Datenschutzes insbesondere aus dem Blickwinkel eines Datenschutzbeauftragten vermitteln und dabei Tipps geben für die Organisation von dessen Arbeit mit einer spezifischen Schwerpunktsetzung auf den Datenschutz im Krankenhaus. Dadurch, dass die Themen Internetpräsenz und IT-Sicherheit behandelt werden, werden auch im Gesundheitsbereich auftretende, nicht gesundheitsspezifische Fragen behandelt, dies aber nicht umfassend: So fehlt z. B. der Beschäftigtendatenschutz fast vollständig. Es genügt also nicht, allein auf dieses Werk zu vertrauen, zumal auch die weiterführenden Hinweise eher rar sind. Geeignet ist es dagegen gut für Schulungszwecke und als Einführung sowie als erste Orientierung.



Däubler, Wolfgang
SÜG Sicherheitsüberprüfungsgesetz
Kommentar
C.H.Beck München, 2019,
ISBN 978-406-72851-8, 303 S., 79 €

(tw) In unsicheren Zeit, in denen wir leben, ist Arbeitnehmerdatenschutz oft eine Frage der Abwägung mit Sicherheitsinteressen. Zum Schutz vor Sabotage und Spionage, aber auch generell zur Gewährleistung der Zuver-

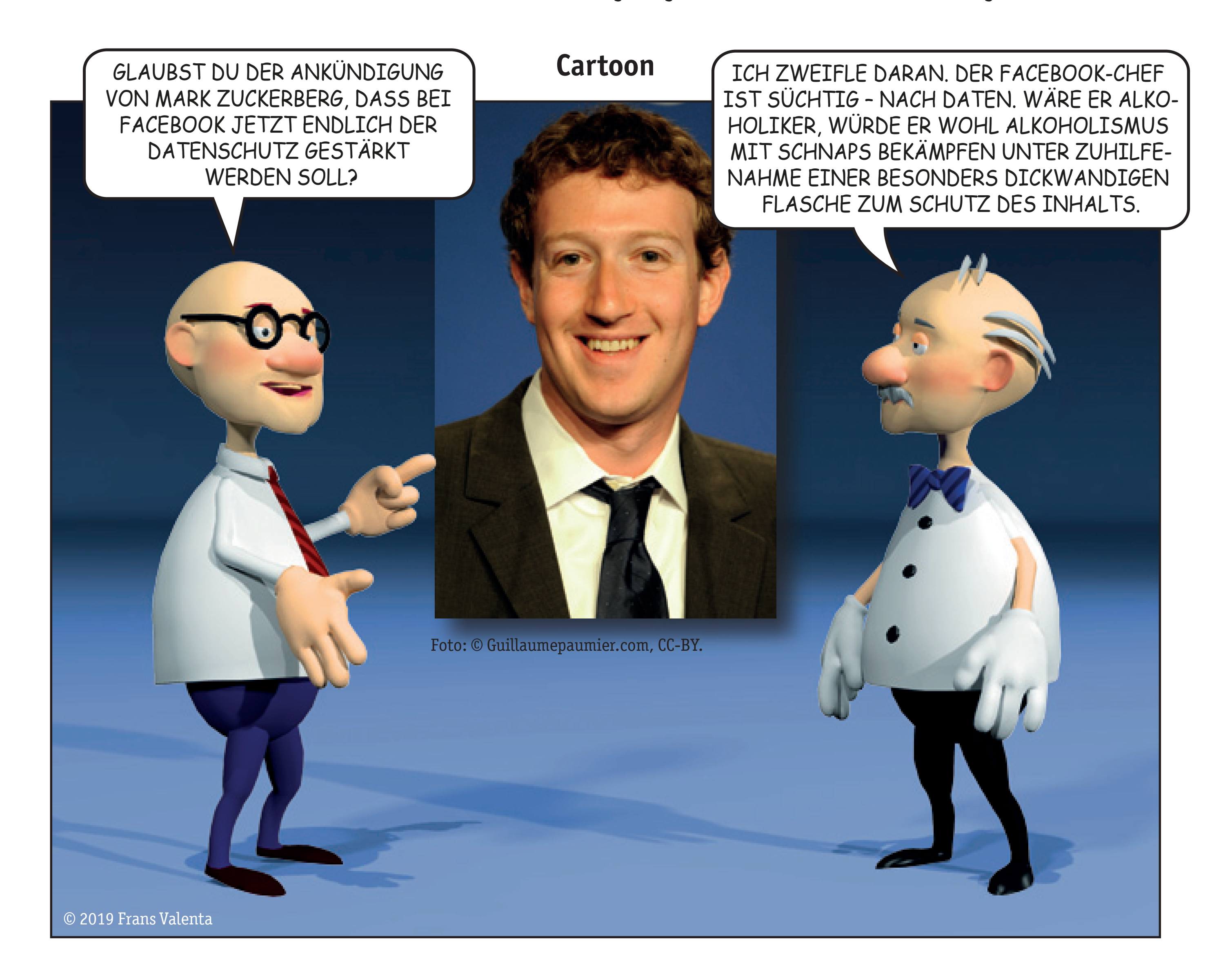
lässigkeit in Sachen Sicherheit gibt es Sicherheitsüberprüfungen, bei denen die Beschäftigten oder Bewerbenden auf ihre sicherheitspolitische Geschichte hin durchleuchtet werden. Bei dieser Durchleuchtung spielen neben den jeweiligen öffentlichen und privaten Arbeitgebern vor allem Sicherheitsbehörden und insbesondere auch Geheimdienste mit ihren oft nur vage fundierten Erkenntnissen eine zentrale Rolle.

Da diese Durchleuchtung eine hochsensible personenbezogene Datenverarbeitung ist, bei der für die Betroffenen teilweise existenzielle Entscheidungen getroffen werden, ist das Thema aus Datenschutzsicht von hoher Relevanz. Dies gilt auch, weil Aspekte des Persönlichkeitsschutzes sowohl in der Praxis als auch von Gerichten eher defensiv behandelt werden gemäß dem Motto „Sicherheit first".

Die Gesetze zur Sicherheitsüberprüfung sehen grundsätzlich einen Ausgleich der Interessen vor, so wie dies auch verfassungsrechtlich gefordert wird. Es ist also wichtig, bei der Anwendung der Gesetze sowohl die berechtigten Sicherheitsbelange als auch die des Datenschutzes zur Geltung zu bringen. Hierzu liefert Wolfgang Däubler, der sich als Arbeitsrechtler wie auch als Datenschützer schon seit Jahren einen Namen macht, eine ausführliche und ins Detail gehende Anleitung. Im Vordergrund steht die Kommentierung des Sicherheitsüberprüfungsgesetzes (SÜG) des Bundes, doch sind die Ausführungen auf die Länder-SÜG übertragbar. Kursorisch werden die SÜG von Bayern, Baden-Württemberg, Hessen, Niedersachsen und Nordrhein-Westfalen mitbehandelt. Dargestellt werden auch die Regelungen aus dem Atom- und dem Luftverkehrsrecht sowie sonstiges Gesetzesrecht, etwa das BDSG, das mit zur Anwendung kommt. Auf untergesetzliche Normen, denen in der Praxis eine hohe Relevanz zukommt, wird mit Internetfundstellen verwiesen.

Däubler erschließt mit seinem Kommentar eine Materie, zu der es wenig Literatur gibt. Er liefert eine aktuelle Momentaufnahme, gibt einen Überblick und erschließt das, was hierzu verfasst wurde. Dabei nimmt er eine kritische bürgerrechtliche Haltung ein und betet nicht einfach das nach, was von Regierungen vorgebetet wird. Für Anwälte, Arbeitsgerichte, Personalabteilungen und Sicherheitsbeauftragte, Betriebsrate sowie Beschäftigte in einem sicherheitsüberprüften Bereich ist das Werk eine hilfreiche Unterstützung, um dem Datenschutz Geltung zu schaffen.

Cartoon



So vermeiden Terroristen Fingerabdrücke:



Die EU hat am 04.04.2019 beschlossen, die Daten von Fingerabdrücken für alle neu auszustellenden Personalausweise verbindlich vorzuschreiben.

Die Aufnahme von Fingerabdrücken im Personalausweis war in der Bundesrepublik Deutschland bisher freiwillig.

Einen Zwang dazu gab es schon mal zur Zeit des Nationalsozialismus durch die Verordnung über Kennkarten vom 22. Juli 1938 (RGBl. I S. 913) als „allgemeiner polizeilicher Inlandausweis".